511, 751

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003 年11 月6 日 (06.11.2003)

PCT

(10) 国際公開番号
WO 03/091862 A1

(51) 国際特許分類[7]: G06F 1/00, 9/445

(21) 国際出願番号: PCT/JP03/04808

(22) 国際出願日: 2003 年4 月16 日 (16.04.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-120430 2002 年4 月23 日 (23.04.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市 大字門真１００６番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 前田 卓治 (MAEDA,Takuji) [JP/JP]; 〒572-0052 大阪府 寝屋川市 上神田２丁目２０番１−５０１号 Osaka (JP). 三浦 康史 (MIURA,Kouji) [JP/JP]; 〒580-0016 大阪府 松原市 上田３丁目４番１号 Osaka (JP). 徳田 克己 (TOKUDA,Katsumi) [JP/JP]; 〒563-0038 大阪府 池田市 荘園１丁目１３番２号 Osaka (JP). 井上 信治 (INOUE,Shinji) [JP/JP]; 〒572-0081 大阪府 寝屋川市 東香里園町９番１３−３０６号 Osaka (JP).

(74) 代理人: 新居 広守 (NII,Hiromori); 〒532-0011 大阪府 大阪市淀川区 西中島3丁目11番26号 新大阪末広センタービル3F 新居国際特許事務所 Osaka (JP).

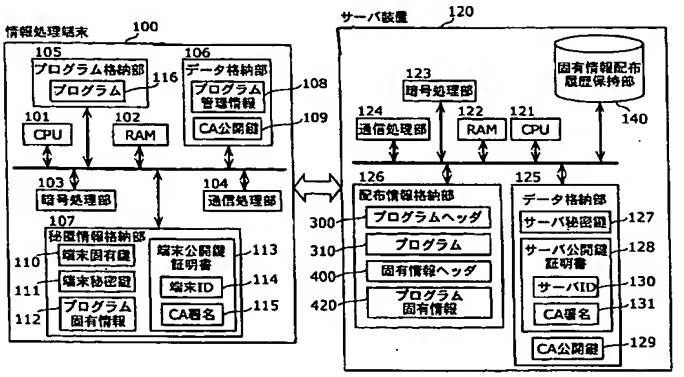
(81) 指定国 (国内): CN, KR, US.

(84) 指定国 (広域): ヨーロッパ特許 (DE, GB).

[続葉有]

(54) Title: SERVER DEVICE AND PROGRAM MANAGEMENT SYSTEM

(54) 発明の名称: サーバ装置及びプログラム管理システム



100...INFORMATION PROCESSING TERMINAL
105...PROGRAM STORAGE UNIT
116...PROGRAM
106...DATA STORAGE UNIT
108...PROGRAM MANAGEMENT INFORMATION
109...CA PUBLIC KEY
103...ENCRYPTION PROCESSING UNIT
104...COMMUNICATION PROCESSING UNIT
107...SECRET INFORMATION STORAGE UNIT
110...TERMINAL UNIQUE KEY
111...TERMINAL PRIVATE KEY
112...PROGRAM UNIQUE INFORMATION
113...TERMINAL PUBLIC KEY CERTIFICATE
114...TERMINAL ID
115...CA SIGNATURE
120...SERVER DEVICE

140...UNIQUE INFORMATION DISTRIBUTION HISTORY HOLDING UNIT
123...ENCRYPTION PROCESSING UNIT
124...COMMUNICATION PROCESSING UNIT
126...DISTRIBUTION INFORMATION STORAGE UNIT
300...PROGRAM HEADER
310...PROGRAM
400...UNIQUE INFORMATION HEADER
420...PROGRAM UNIQUE INFORMATION
125...DATA STORAGE UNIT
127...SERVER PRIVATE KEY
128...SERVER PUBLIC KEY CERTIFICATE
130...SERVER ID
131...CA SIGNATURE
129...CA PUBLIC KEY

(57) Abstract: A server device (120) comprises a CPU (121); a RAM (122); an encryption processing unit (123) that performs encryption and decryption processing; a communication processing unit (124) that performs communication with an information processing terminal (100); a data storage unit (125) in which information that need not be kept secret is stored; a distribution information storage unit (126) in which information on a program to be distributed and so on is stored; and a unique information distribution history holding unit (140) that holds a unique information distribution history (600) used to manage the history of program unique information on a program previously distributed to the information processing terminal (100).

[続葉有]

WO 03/091862 A1

添付公開書類:
— 国際調査報告書
— 補正書・説明書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

サーバ装置（１２０）は、ＣＰＵ（１２１）、ＲＡＭ（１２２）、暗号化及び復号化処理を行う暗号処理部（１２３）、情報処理端末（１００）との通信を行う通信処理部（１２４）、秘匿する必要がない情報を格納するデータ格納部（１２５）、配布するプログラムなどの情報を格納する配布情報格納部（１２６）、及び情報処理端末（１００）に以前に配布したプログラムのプログラム固有情報の履歴を管理するための固有情報配布履歴（６００）を保持する固有情報配布履歴保持部（１４０）を有する。

明 細 書

サーバ装置及びプログラム管理システム

技術分野

本発明は、情報処理端末で動作するプログラムの配布を行うサーバ装置、及びサーバ装置と情報処理端末からなるプログラム管理システムに関し、特に不正なプログラムの使用を図る情報処理端末の排除における技術に関する。

背景技術

近年のネットワークの発展に伴い、ネットワークを経由して商取引を行う電子商取引システム（Electronic commerce system）、映画、音楽等のコンテンツの配信を行うコンテンツ配信システムが多く発表されている。これらのシステムにおいては、ネットワークを介して接続される機器間で、コンテンツの利用権利、課金に使用する鍵等の価値ある情報データのみでなく、音楽プレーヤプログラム等のプログラム自体を交換することも可能である。また、このようなプログラムの交換は、従来のＰＣ以外にも携帯電話等の組込み機器においても実現されることが予測される。

そして、電子ショッピングやコンテンツ配信サービスなど、課金を伴う商用システムをネットワークを介して実現する場合においては、悪意のあるユーザが不正にプログラムを書き換えることが可能であれば、課金情報の操作により無料で商品やコンテンツを購入するなどの不正行為が行われる危険性がある。そのため、ネットワーク経由のプログラム更新による不具合修正や追加を行う場合、悪意のあるユーザの不正使用を

防止するために、プログラムの正当性を検証する必要がある。

従来プログラムの正当性を検証する方法としては、電子的な署名を用いる方法が存在する(例えば、特開２０００－３３９１５３号公報参照)。この方法では、公開鍵暗号方式と呼ばれる２つの対となる鍵の組を用いた暗号化データ交換方式を利用する。図２０は、この電子的な署名を用いたプログラムの正当性検証方法に関する説明図である。

プログラム発行者２０００は、プログラム発行の身元を確認し、保証する第三者機関である認証局（ＣＡ：Certification Authority）２０１０に公開鍵２００１を送付する。その後、認証局２０１０は、プログラム発行者２０００の身元を確認、審査する。認証局２０１０がプログラム発行者２０００を信頼できると判断した場合、プログラム発行者２０００の公開鍵２００１に対しＣＡ秘密鍵２０１２で電子的な署名を行った証明書２００３を発行する。証明書２００３は公開鍵保有者の身元を識別する情報を含み、認証局２０１０が公開鍵保有者の身元を保証するものである。そして、認証局２０１０は、プログラム発行者２０００に公開鍵証明書２００３を送付する。

プログラム発行者２０００は、ユーザ２０２０に配布するプログラムに対し、自己の秘密鍵２００２で電子的な署名を行い、公開鍵証明書２００３、及び署名付きプログラム２００４を配布する。

ユーザ２０２０は、認証局２０１０からＣＡ公開鍵２０１１を取得し、ＣＡ公開鍵２０１１を用いてプログラム発行者の公開鍵証明書２００３の署名を検証する。署名の検証が正しく行われた場合、公開鍵証明書２００３に含まれる公開鍵２００１を用いて署名付きプログラム２００４の署名を検証する。この署名の検証が正しく行われた場合、配布されたプログラムがプログラム発行者２０００から配布されたプログラムであり、改ざんされていないことを検証できる。

従って、この正当性検証方式においては、プログラムにプログラム発行者２０００の電子的な署名を付加することによりプログラムの正当性を保証して、ユーザ２０２０は取得したプログラム２０２１がプログラム発行者２０００から正当に配布されたものであることを検証できる。

しかし、図２０に示す正当性検証方式においては、配布時におけるプログラムの正当性検証は行えるが、配布後の情報処理端末におけるプログラムに関して正当性を保証することはできない。尚、公開鍵暗号方式及び証明書、署名、認証の仕組みに関しては、種々の文献（例えば、「Ａｐｐｌｉｅｄ　Ｃｒｙｐｔｏｇｒａｐｈｙ」Ｂｒｕｃｅ　Ｓｃｈｎｅｉｅｒ，Ｊｏｈｎ　Ｗｉｌｅｙ　＆　Ｓｏｎｓ，Ｉｎｃ（１９９６）参照）に詳細が記されている。

この問題点を解決する方法として、プログラム配布先のユーザ識別子を用いてプログラム配布元でプログラムを暗号化して配布し、ユーザは使用時にユーザ識別子を用いてプログラムを復号化して実行する方法がある（例えば、特開平７－２９５８００号公報参照）。この方法では、万が一プログラムが不正にコピーされたとしても、ユーザ識別子が一致しなければプログラムを復号し実行することができないため、不正コピー、不正改ざんを防止することが可能となる。

また、プログラムの配布装置としては、プログラムの配布に当たって配布の妥当性をプログラムのコピー数とコピー許可数の差により判定して、無制限な配布が行われることを物理的に防ぐことができ、プログラムコピーに関する使用契約を物理的に尊守させる配布装置が開示されている（例えば、特公平６－８７２２０号公報参照）。

この発明においては、プログラム配布装置は、プログラム毎に情報処理装置の配布先を記憶して、コピー許可数とコピー数とによりプログラムを配布するプログラム配布装置とすることが可能となる。

一方、ネットワークを用いた電子ショッピングやコンテンツ配信サービス等の課金を伴う商用システムを実現する場合、ユーザに対する課金を行うため、ユーザを特定する方法が必要となる。この方法の１つとして、プログラムあるいはプログラムと共に配布する情報の中に、ユーザ毎に割り当てるＩＤや鍵などの固有情報を含ませる場合がある。この場合、ユーザ毎に固有情報を割り当て、プログラム配布元のサーバ装置側において固有情報を管理することで、ユーザが不正行為を行った際において固有情報を元にユーザを特定することが可能となる。

図２１は、従来の情報処理端末２１０１とサーバ装置２１０２及び２１０３との間のプログラム管理システムの参考図である。尚、図２１においては説明のためにアプリケーションデータ用のサーバ装置２１０３及びプログラム用のサーバ装置２１０２に分けて示す。

情報処理端末２１０１は、プログラム配布元となるサーバ装置２１０２から、例えば好みの音楽データをダウンロードして再生可能な音楽プレーヤプログラムを取得する。この音楽プレーヤプログラムには固有情報「０１０１」が含まれるとする。尚、プログラムの安全な配布を図るために、通信路はＳＳＬ（Secure Socket Layer）を用いて暗号化し、盗聴等のハッキング行為を防止する。

情報処理端末２１０１の利用者が音楽データ等の取得を要求する際においては、情報処理端末２１０１から前記固有情報「０１０１」が付与された音楽データ取得要求をアプリケーション用のサーバ装置２１０３に送信する。そして、サーバ装置２１０３は、不正な音楽プレーヤプログラムが実行される情報処理端末を排除するための無効化リスト（ＣＲＬ：certificate revocation list）を有しており、情報処理端末２１０１から音楽データ取得要求に合わせて送信される固有情報「０１０１」がＣＲＬに記載されているため情報処理端末２１０１に音楽データの送

信を行わない。尚、ＣＲＬに固有情報が記載されていない場合においては要求される音楽データを情報処理端末２１０１に送る。

このように、不正なプログラム使用を行っている情報処理端末２１０１の有するプログラムの固有情報を特定すれば、ＣＲＬを用いて不正使用を図る情報処理端末２１０１を排除することが可能となる。

尚、サーバ装置２１０２等から情報処理端末２１０１にダウンロードされるデータに電子的な署名を付加して、情報処理端末２１０１側で署名検証を行うことにより、ダウンロードデータの改ざん、すり替え、盗聴等を防止して、不正行為からダウンロードデータを守る安全な配布も可能となる。

しかしながら、上述したプログラム配布元において各ユーザ識別子に応じたプログラム暗号処理を行う方法においては、プログラム配布元にかかる処理の負担が大きくなるという問題が生じる。

また、上述したプログラム配布装置がプログラム毎に情報処理装置の配布先を記憶して、コピー許可数とコピー数とによりプログラムを配布する方法は、プログラム配布装置はプログラムの配布要求毎に配布先の装置のＩＤを確認してコピー許可数に従ってプログラムを配布するものであり、プログラムの不正使用を防止するものではない。

さらに、図２１に示すサーバ装置２１０３がプログラムの固有情報を記載したＣＲＬを用いて不正利用を図る情報処理端末２１０１の排除を行う方法においては、情報処理端末２１０１が不正にデータを取得しようと試み、サーバ装置２１０３のＣＲＬにより不正端末としてデータ取得を排除される場合においても、情報処理端末２１０１の使用者が、別の固有情報のダウンロードをサーバ装置２１０２から行いプログラムの固有情報を新たな固有情報に更新することによりサーバ装置２１０３のＣＲＬを用いた排除から回避することが可能となるという問題がある。

本発明は以上のような課題に鑑みてなされたものであり、プログラム配布元であるサーバ装置において、固有情報を用いたリストにより排除された不正な情報処理端末が新規な固有情報を取得して排除を回避することを防止するサーバ装置を提供することを第１の目的とする。また、情報処理端末へのプログラム配信においてサーバ装置の処理負担を少なくすることをも目的とする。

そして、サーバ装置と情報処理端末との間においてプログラムの配布を行うプログラム管理システムにおいても、不正な情報処理端末からの新規な固有情報の取得要求を排除して情報処理端末でのプログラムの不正使用を防ぐことが可能なプログラム管理システムを提供することを目的とする。

発明の開示

前記課題を解決するために、本発明に係るサーバ装置は、外部から書き換えが行えない端末ＩＤを保持する情報処理端末とネットワークを介して接続され前記情報処理端末で動作するプログラムを保持するサーバ装置であって、以前に配布したプログラムと端末ＩＤとの関連を示すテーブルを保持するテーブル保持手段と、前記テーブルを参照して、前記情報処理端末から送信され前記端末ＩＤを伴うプログラム取得要求に対するプログラムの配布の当否を判定する判定手段とを備えることを特徴とする。

また、本発明に係るサーバ装置から情報処理端末に配布されるプログラムには、前記情報処理端末で動作するプログラム本体及び前記プログラム本体に使用される固有の情報であるプログラム固有情報が含まれ、前記判定手段は、前記プログラム取得要求に付与されている前記端末ＩＤが前記テーブルに記録されている場合には、前記プログラム固有情報

の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、前記端末ＩＤが前記テーブルに記載されていない場合には、前記端末ＩＤと前記プログラム固有情報とを対応させて前記テーブルに追加すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定することを特徴とする。

これらにより、サーバ装置は、情報処理端末が以前に配布したプログラムに対応するプログラム固有情報の新規取得を防止することが可能となり、新たなプログラム固有情報を取得して排除の回避を図る情報処理端末の不正行為を確実に防止することが可能となる。

そして、前記課題を解決するために、本発明に係るプログラム管理システムは、外部から書き換えが行えない端末ＩＤを保持する情報処理端末と、当該情報処理端末とネットワークを介して接続され前記情報処理端末で動作するプログラムを保持するサーバ装置とから構成されるプログラム管理システムであって、前記情報処理端末は、前記プログラムの取得を要求する場合には、前記端末ＩＤを付与したプログラム取得要求を前記サーバ装置に送信し、前記サーバ装置は、前記プログラム取得要求を受信して、以前に配布したプログラムと端末ＩＤとの関連を示すテーブルを保持するテーブル保持手段と、前記テーブルを参照して、前記情報処理端末から送信されて前記端末ＩＤが付与されているプログラム取得要求に対するプログラムの配布の当否を判定する判定手段とを備えることを特徴とする。

このように、本発明は、上述のようなサーバ装置として実現できるのみではなく、サーバ装置と情報処理端末との間のプログラム管理システムやサーバ装置が備える手段をステップとするプログラム配布方法としても実現できる。また、このプログラム配布方法をコンピュータ等で実現させるプログラムとして実現したり、当該プログラムをＣＤ－ＲＯＭ

等の記録媒体や通信ネットワーク等の伝送媒体を介して流通させることができるのは言うまでもない。

図面の簡単な説明

図１は、実施の形態１における情報処理端末とサーバ装置との構成図を示している。

図２は、本実施の形態１に係るサーバ装置から情報処理端末側に送信されるプログラム全体の構成図である。

図３（ａ）は、プログラムヘッダに格納される情報の一例を示す図である。

図３（ｂ）は、プログラムに格納される情報の一例を示す図である。

図４（ａ）は、固有情報ヘッダに格納される情報の一例を示す図である。

図４（ｂ）は、プログラム固有情報に格納される情報の一例を示す図である。

図５は、情報処理端末とサーバ装置と間で行われるプログラム更新システムにおける動作手順を示す図である。

図６は、固有情報配布履歴保持部に保持される固有情報配布履歴の情報格納の一例を示す図である。

図７は、サーバ装置におけるプログラムの配布手順を示すフローチャートである。

図８は、本実施の形態１に係るサーバ装置を用いたプログラム管理システムを示す全体図である。

図９は、本実施の形態１に係るプログラムヘッダとプログラムに含まれる別のデータ構造を示す図である。

図１０は、固有情報ヘッダとプログラム固有情報とに含まれる別のデ

一タ構造を示す図である。

図１１は、本発明の実施の形態２に係る情報処理端末とサーバ装置との構成図を示す。

図１２（ａ）は、本実施の形態２に係る固有情報配布履歴に含まれる情報の一例を示す図である。

図１２（ｂ）は、本実施の形態２に係るプログラム／固有情報対応表に含まれる情報の一例を示す図である。

図１３は、サーバ装置におけるプログラムの配布手順を示すフローチャートである。

図１４は、本実施の形態３に係る情報処理端末とサーバ装置の構成図を示す。

図１５は、本実施の形態３に係る配布回数情報の情報格納例を示す図である。

図１６は、サーバ装置におけるプログラムの配布手順を示すフローチャートである。

図１７は、本実施の形態４に係る情報処理端末とサーバ装置の構成図を示す。

図１８（ａ）は、本実施の形態４に係る配布回数情報に格納されるデータの一例を示す図である。

図１８（ｂ）は、本実施の形態４に係るプログラム／固有情報対応表に格納されるデータの一例を示す図である。

図１９は、サーバ装置におけるプログラムの配布手順を示すフローチャートである。

図２０は、従来の電子的な署名を用いたプログラムの正当性検証方法に関する説明図である。

図２１は、従来の情報処理端末とサーバ装置との間のプログラム管理

システムの参考図である。

発明を実施するための最良の形態

以下、本発明の実施の形態に係るサーバ装置及びプログラム管理システムについて図面を用いて説明する。

（実施の形態１）

図１は本発明の実施の形態１における情報処理端末１００とサーバ装置１２０との構成図を示している。

情報処理端末１００は、サーバ装置１２０から取得した電子商取引やコンテンツ配信等に用いられるプログラムを使用する端末装置であり、ＣＰＵ１０１、ＲＡＭ１０２、プログラムやデータ等の暗号化及び復号化処理を行う暗号処理部１０３、サーバ装置１２０との通信を行う通信処理部１０４、プログラムを格納するプログラム格納部１０５、ＣＡ公開鍵など特に秘匿する必要がない情報を格納するデータ格納部１０６、及び秘密鍵など秘匿する必要がある情報を格納する秘匿情報格納部１０７から構成されている。

プログラム格納部１０５は、ＣＰＵ１０１で動作するプログラム１１６を格納する。

データ格納部１０６は、情報処理端末１００で使用されるデータのうち特に秘匿する必要がないものを格納すると共に、情報処理端末１００に格納されているプログラムのＩＤやバージョン番号など格納プログラムの管理情報であるプログラム管理情報１０８及びＣＡ公開鍵１０９を格納する。

また、秘匿情報格納部１０７は、情報処理端末１００内で秘匿する必要がある情報を格納しており、情報処理端末毎に異なる鍵である端末固有鍵１１０、情報処理端末毎に異なる公開鍵ペアの１つである端末秘密

鍵１１１、プログラムが使用する固有鍵などのプログラム固有情報１１２、情報処理端末毎に異なる公開鍵ペアの他方である端末公開鍵証明書１１３を格納する。そして、端末公開鍵証明書１１３は情報処理端末１００を一意に識別するＩＤである端末ＩＤ１１４、端末公開鍵証明書１１３に対し認証局が付加したＣＡ署名１１５を含んでいる。

一方、本発明に係るサーバ装置１２０は、情報処理端末１００から要求されるプログラムを配布する装置であり、ＣＰＵ１２１、ＲＡＭ１２２、プログラムやデータなどの暗号化及び復号化処理を行う暗号処理部１２３、情報処理端末１００との通信を行う通信処理部１２４、ＣＡ公開鍵など特に秘匿する必要がない情報を格納するデータ格納部１２５、情報処理端末１００に配布するプログラムなどの情報を格納する配布情報格納部１２６、及び固有情報配布履歴保持部１４０とから構成されている。

そして、本発明に係るサーバ装置１２０は、固有情報配布履歴保持部１４０を有することを特徴としている。この固有情報配布履歴保持部１４０は、情報処理端末１００に配布したプログラムのプログラム固有情報の履歴を管理するための固有情報配布履歴６００を保持している。

データ格納部１２５は、サーバ装置１２０が使用する情報を格納する領域であり、公開鍵ペアの１つであるサーバ秘密鍵１２７、公開鍵ペアの他方であるサーバ公開鍵証明書１２８、及びＣＡ公開鍵１２９を格納する。サーバ公開鍵証明書１２８は、サーバを一意に識別するＩＤであるサーバＩＤ１３０、サーバ公開鍵証明書に対しＣＡが付加したＣＡ署名１３１を含んでいる。配布情報格納部１２６は、サーバ装置１２０が情報処理端末１００に対して配布する情報を格納する領域であり、プログラムヘッダ３００、プログラム３１０、固有情報ヘッダ４００、及びプログラム固有情報４２０を格納する。尚、この配布情報であるプログ

ラム全体の図は後述の図２に示す。

配布情報格納部１２６に格納されているプログラムヘッダ３００、プログラム３１０、固有情報ヘッダ４００、及びプログラム固有情報４２０には第三者認証機関であるＣＡ署名が付加されており、このＣＡ署名により配布情報が正当な配布元から配布されるものであることを保証する。

図２は、本実施の形態１に係るサーバ装置１２０から情報処理端末１００側に送信されるプログラム全体２００の構成図である。このプログラムの全体２００はサーバ装置１２０の配布情報格納部１２６に格納される情報であり、本実施の形態１においては、プログラムヘッダ３００、プログラム３１０、固有情報ヘッダ４００及びプログラム固有情報４２０より構成される。また、本発明においては、プログラム全体２００をプログラム３１０及びプログラム固有情報４２０に分離し、さらに、ヘッダ部とデータ部とに分離することを特徴としている。

尚、本実施の形態に係るプログラム管理システムにおいては、情報処理端末１００がプログラム３１０で使用するアプリケーションデータをサーバ装置１２０等から取得する場合においては、アプリケーションデータ取得要求にプログラム固有情報４２０を付与して送信する。このことにより、サーバ装置１２０等が有するプログラム固有情報４２０を用いたＣＲＬにより不正な情報処理端末を排除することが可能となる。

図３（ａ）及び（ｂ）は、プログラムヘッダ３００及びプログラム３１０に格納される情報の一例を示す図である。

プログラムヘッダ３００は、プログラム３１０に関する情報を格納するものであり、次の情報を含む。

（１）プログラムヘッダ３００が格納する情報がどのプログラム３１０に対応する情報かを示すプログラムＩＤ（３０１）。（２）対応する

プログラム３１０のバージョン番号（３０２）。（３）対応するプログラム３１０のプログラムサイズ（３０３）。（４）対応するプログラム３１０のハッシュ値（３０４）。（５）前記（１）から（４）までの情報を含むプログラムヘッダ３００全体に対するＣＡ署名（３０５）。

また、プログラム３１０には、プログラム３１０に対するＣＡ署名（３１１）が付加されている。このように、プログラムヘッダ３００及びプログラム３１０は共にＣＡ署名３０５及び３１１を含むため、情報処理端末１００においてプログラムヘッダ、プログラムが正当な配布元から配布されたものであることを検証することが可能である。

図４（ａ）及び（ｂ）は、固有情報ヘッダ４００及びプログラム固有情報４２０に格納される情報の一例を示す図である。

固有情報ヘッダ４００は、プログラム固有情報４２０に関する情報を格納するものであり、次の情報を含む。

（１）固有情報ヘッダ４００が格納する情報がどのプログラム固有情報４２０に対応した情報かを示すプログラム固有情報ＩＤ（４０１）。（２）対応するプログラム固有情報４２０を使用するプログラム３１０のプログラムＩＤ（４０２）。（３）対応するプログラム固有情報４２０が格納する固有情報の数（４０３）。（４）対応するプログラム固有情報４２０全体のサイズ（４０４）。（５）対応するプログラム固有情報４２０に含まれる個々の固有情報に関する情報を示す固有情報サブヘッダ（４０５）。固有情報サブヘッダ４０５はプログラム固有情報４２０に含まれる個々の固有情報の数（１～ｎ）だけ存在する。（６）前記（１）から（５）までの情報を含む固有情報ヘッダ４００全体に対するＣＡ署名（４０６）。

固有情報サブヘッダ４０５は、さらに個々の固有情報を識別するためのＩＤであるプログラム固有情報サブＩＤ４１１、個々の固有情報のサ

イズ４１２から構成される。

また、プログラム固有情報４２０は、複数のプログラム固有情報（４２１）と、プログラム固有情報全体に対するＣＡ署名（４２２）を含む。このため、固有情報ヘッダ４００、プログラム固有情報４２０は共にＣＡ署名（４０６及び４２２）を含むため、情報処理端末１００において固有情報ヘッダ４００、プログラム固有情報４２０が正当な配布元から配布されたものであることを検証することが可能である。

次に情報処理端末１００とサーバ装置１２０との間で行われるプログラム更新システムにおける動作手順の例を、図５を用いて説明する。このプログラム更新システムにおいて、情報処理端末１００は、まず、ヘッダ取得要求を行い、空き領域の確認を行う。また、サーバ装置１２０においては、固有情報配布履歴保持部１４０から固有情報配布履歴６００を参照することにより、プログラムの不正使用を図る情報処理端末１００を排除することが可能となる。

最初に、情報処理端末１００はサーバ装置１２０とＳＳＬによる接続を行う（Ｓ５０１）。この際、サーバ装置１２０は情報処理端末１００の端末ＩＤの取得を行う。尚、ＳＳＬは、２点間でデータを安全に送受信するために、公開鍵暗号方式と秘密鍵暗号方式を併用して、データを暗号化して送受信する仕組みである。また、ＳＳＬではセッション鍵と呼ばれるそのセッションでのみ有効な鍵を共有するため、図５に示すＳ５０２以降の情報処理端末１００とサーバ装置１２０間のデータ送受信は、すべてセッション鍵を用いた暗号化データにより行われるものとする。

次に、情報処理端末１００はサーバ装置１２０に対し、取得したいプログラム３１０のプログラムＩＤを指定してヘッダ取得要求を行う（Ｓ５０２）。この際、サーバ装置１２０は、固有情報配布履歴保持部１４

０に保持されている固有情報配布履歴６００により、端末ＩＤとプログラム固有情報ＩＤとの対応関係を確認する。つまり、情報処理端末１００に対して、固有情報ＩＤを既に配布したかどうかを確認する。そして、正規の情報処理端末からのヘッダ取得要求であると判断する場合においては、ヘッダ取得要求を受信したサーバ装置１２０は、配布情報格納部１２６に格納したプログラムヘッダ３００を情報処理端末１００に送信する（Ｓ５０３）。

そして、サーバ装置１２０からプログラムヘッダ３００を受信した情報処理端末１００は、データ格納部１０６に格納しているＣＡ公開鍵１０９を用いて、プログラムヘッダ３００に含まれているＣＡ署名を検証する（Ｓ５０４）。これにより、情報処理端末１００はプログラムヘッダ３００が改ざんされていない正当な配布元から配布された情報であることを検証する。また、プログラムヘッダ３００には、プログラムのプログラムＩＤ３０１、バージョン番号３０２、サイズ３０３、プログラムのハッシュ値３０４などプログラムに関する情報が格納されているため、情報処理端末１００は、これらの情報と、データ格納部１０６に格納されているプログラム管理情報１０８内に記載されているプログラムＩＤ、バージョン情報、空き容量情報を比較し、更新対象のプログラム３１０が正しくサーバ装置１２０から配布されたか、プログラム３１０を格納する空き容量が存在するか確認する（Ｓ５０４）。このため、本実施の形態１に係る情報処理端末１００はプログラム３１０のダウンロード中にプログラムの取得不可となるような弊害を防止する。

次に、サーバ装置１２０は配布情報格納部１２６に格納した固有情報ヘッダ４００を情報処理端末１００に送信する（Ｓ５０５）。

そして、サーバ装置１２０から固有情報ヘッダ４００を受信した情報処理端末１００は、データ格納部１０６に格納しているＣＡ公開鍵１０

９を用いて、固有情報ヘッダ４００に含まれているＣＡ署名を検証する（Ｓ５０６）。これにより、情報処理端末１００は固有情報ヘッダ４００が改ざんされていない、正当な配布元から配布された情報であることを検証する。固有情報ヘッダ４００には、プログラム固有情報４２０を一意に識別するプログラム固有情報ＩＤ４０１、プログラム固有情報に関連するプログラムのプログラムＩＤ４０２、プログラム固有情報で配布される情報に含まれる固有情報の数４０３、サイズ４０４などプログラム固有情報４２０に関する情報が格納されているため、情報処理端末１００は、これらの情報と、データ格納部１０６に格納されているプログラム管理情報１０８内に記載されているプログラムＩＤ、空き容量情報を比較し、更新対象のプログラム３１０に関するプログラム固有情報４２０が正しくサーバ装置１２０から配布されたか、プログラム固有情報４２０を格納する空き容量が存在するかプログラム３１０のダウンロードの前に確認する（Ｓ５０６）。

そして、情報処理端末１００は、プログラム３１０、プログラム固有情報４２０の取得が行えると判断した場合、サーバ装置１２０に対しプログラムＩＤを指定してプログラム取得要求を行う（Ｓ５０７）。

そして、プログラム取得要求を受信したサーバ装置１２０は、配布情報格納部１２６に格納したプログラム３１０を情報処理端末１００に送信する（Ｓ５０８）。サーバ装置１２０からプログラム３１０を受信した情報処理端末１００は、データ格納部１０６に格納しているＣＡ公開鍵１０９を用いて、プログラム３１０に含まれているＣＡ署名を検証する（Ｓ５０９）。これにより、情報処理端末１００はプログラム３１０が改ざんされていない、正当な配布元から配布された情報であることを検証する。取得データの正当性が検証できた場合、取得したプログラム３１０を秘匿情報格納部１０７に格納している端末固有鍵１１０で暗号

化し、プログラム格納部１０５に格納する（Ｓ５０９）。その際、プログラム格納位置やプログラムＩＤ、バージョン番号などをプログラム管理情報１０８に格納し、プログラムの管理を行う。

次に、プログラムの格納が完了した後、プログラム格納部１０５に格納したプログラム１１６を、端末固有鍵１１０を用いて復号し、ハッシュ値を算出する。算出した値とプログラムヘッダ３００に格納されているハッシュ値の比較を行い、プログラムが正しく格納されていることを確認する（Ｓ５１０）。

次に、情報処理端末１００はサーバ装置１２０に対しプログラムＩＤを指定してプログラム固有情報取得要求を行う（Ｓ５１１）。

そして、サーバ装置１２０は配布情報格納部１２６に格納したプログラム固有情報４２０を情報処理端末１００に送信する（Ｓ５１２）。サーバ装置１２０からプログラム固有情報４２０を受信した情報処理端末１００は、データ格納部１０６に格納しているＣＡ公開鍵１０９を用いて、プログラム固有情報４２０に含まれているＣＡ署名を検証する（Ｓ５１３）。これにより、情報処理端末１００はプログラム固有情報が改ざんされていない、正当な配布元から配布された情報であることを検証する。取得データの正当性が検証できた場合、取得したプログラム固有情報を秘匿情報格納部１０７に格納する（Ｓ５１３）。

最後に、情報処理端末１００におけるプログラム、プログラム固有情報の格納が完了した後、情報処理端末１００とサーバ装置１２０との間の通信を切断する（Ｓ５１４）。

このように、本実施の形態１に係る情報処理端末１００は、ヘッダ取得要求を行うことによりプログラム３１０を格納する空き容量が存在するか等の確認して、より安全にプログラムのダウンロードを行うことが可能となる。尚、この場合において、プログラム３１０及びプログラム

固有情報４２０のハッシュ値を算出して、算出したハッシュ値と、プログラムヘッダ３００及びプログラム固有情報ヘッダ４００に格納されているハッシュ値とを比較することにより正当な配布情報であることを確認することも考え得る。

図６は、固有情報配布履歴保持部１４０に保持される固有情報配布履歴６００の情報格納の一例を示す図である。

サーバ装置１２０は、以前に情報処理端末１００に配布したプログラムに対応するプログラム固有情報４２０と当該情報処理端末１００の端末ＩＤとを記録したテーブルを固有情報配布履歴６００とする。

そして、サーバ装置１２０は、プログラム固有情報４２０を配布した情報処理端末１００を識別するＩＤである端末ＩＤ６０１、及び配布したプログラム固有情報４２０を識別するＩＤであるプログラム固有情報ＩＤ６０２を固有情報配布履歴保持部１４０に格納する。また、必要に応じてプログラム固有情報４２０を最後に配布した日時を示す最終配布日付６０３を固有情報配布履歴６００に格納する。

図６においては、サーバ装置１２０は情報処理端末１００に５つのプログラム固有情報４２０を配布済みであり、それぞれの端末ＩＤ６０１、プログラム固有情報ＩＤ６０２の組は、（端末ＩＤ，プログラム固有情報ＩＤ）＝（０００１，０００１）、（０００２，０００２）、（００１０，０００３）、（００１５，０００４）、（００２０，０００５）となる。

図７は、サーバ装置１２０におけるプログラム３１０の配布手順を示すフローチャートである。

最初に、サーバ装置１２０は情報処理端末１００からプログラム配布要求を受信する（Ｓ７０１）。次に、サーバ装置１２０は、受信したプログラム配布要求に含まれる情報処理端末１００の端末ＩＤを取得して

（Ｓ７０２）、固有情報配布履歴６００に対して取得した端末ＩＤを検索し（Ｓ７０３）、固有情報配布履歴６００に同じ端末ＩＤが格納されているか否かの判定を行う（Ｓ７０４）。

サーバ装置１２０は、固有情報配布履歴６００に同じ端末ＩＤが格納されていた場合には（Ｓ７０４のＹ）、情報処理端末１００には既にプログラム固有情報４２０を配布済みであるため、プログラム３１０のみを送信し処理を終了する（Ｓ７０８）。

また、サーバ装置１２０は、固有情報配布履歴６００に同じ端末ＩＤが格納されていない場合（Ｓ７０４でＮ）、情報処理端末１００に対しては新たにプログラム固有情報４２０を割り当てて（Ｓ７０５）、この新たに割り当てたプログラム固有情報４２０に関し、端末ＩＤ６０１とプログラム固有情報ＩＤ６０２の対応を追加して固有情報配布履歴６００を更新する（Ｓ７０６）。そして、サーバ装置１２０は、プログラム固有情報４２０を情報処理端末１００に送信し、プログラム３１０を情報処理端末１００に送信して処理を終了する（Ｓ７０８）。

このように、サーバ装置１２０において固有情報配布履歴６００を用いてプログラム固有情報を配布管理することにより、１つの情報処理端末１００へ複数のプログラム固有情報４２０を配布することを確実に防止する。これにより、サーバ装置１２０は、既にＣＲＬ等によりプログラム固有情報４２０を用いて不正端末と認識され、排除されている情報処理端末１００に対しては、新たなプログラム固有情報４２０を割り当てることはない。従って、新たなプログラム固有情報４２０を取得して排除の回避を図る情報処理端末１００の不正行為を防止することが可能となる。

図８は、本実施の形態１に係るサーバ装置１２０を用いたプログラム管理システムを示す全体図である。

プログラム用のサーバ装置１２０ａは、プログラム取得要求に対応するプログラムを情報処理端末１００に送信する。サーバ装置１２０ｂは、情報処理端末１００で動作するプログラムに用いるアプリケーションを情報処理端末１００に送信する。尚、図８においては、情報処理端末１００の保持するプログラムのプログラム固有情報を「０１０１」として、ＣＲＬ８００の排除からの回避を図るために新たなプログラム固有情報の不正取得を図る端末として説明を行う。また、プログラムの安全な配布を図るために、通信路はＳＳＬを用いて暗号化通信路としている。

情報処理端末１００の利用者がアプリケーションデータを要求する際においては、情報処理端末１００の保持するプログラムのプログラム固有情報「０１０１」を付与したアプリケーション取得要求をアプリケーションデータ用のサーバ装置１２０ｂに送信する。

そして、サーバ装置１２０ｂは、プログラム固有情報を用いた不正プログラムの無効化リスト（ＣＲＬ）８００を有しており、情報処理端末１００からの取得要求に付与されるプログラム固有情報「０１０１」がＣＲＬ８００に記載されているためにアプリケーションデータの送信を行わないことで不正な情報処理端末の排除を行う。尚、ＣＲＬにプログラム固有情報が記載されていない場合においては、サーバ装置１２０ｂは、アプリケーションデータを情報処理端末１００に送る。また、サーバ装置１２０ａ等からダウンロードするデータにＣＡ署名を付加して、情報処理端末１００で署名検証を行うことにより、ダウンロードデータの通信路上での改ざん、すり替え、盗聴等を防止する。

プログラム固有情報「０１０１」がＣＲＬ８００に記載された情報処理端末１００のユーザは、新たな別のプログラム固有情報を得てＣＲＬによる排除を回避するためにプログラム用のサーバ装置１２０ａよりプログラム固有情報の取得要求を行う。

このような場合において、本発明に係るサーバ装置１２０ａは、固有情報配布履歴保持部１４０において、以前に配布したプログラムに関し、情報処理端末１００の端末ＩＤ「０１０２」と、プログラム固有情報ＩＤ「０１０１」とを記録した固有情報配布履歴６００を有している。

そして、情報処理端末１００から、新たなプログラム固有情報取得要求をサーバ装置１２０ａに対して行う場合には、サーバ装置１２０ａは、このプログラム固有情報取得要求に付与されている端末ＩＤ「０１０２」が固有情報配布履歴６００に記載されているか否か判断して、記載されている場合においては、プログラム固有情報の配布を禁止してプログラム本体のみの配布を前記情報処理端末１００に行う。尚、固有情報配布履歴６００を参照して、プログラム固有情報取得要求に付与されている端末ＩＤに対応するプログラム固有情報ＩＤが記載されていない場合においては、端末ＩＤとプログラム固有情報ＩＤとを対応させて固有情報配布履歴６００に追加すると共に、プログラムとプログラム固有情報とを情報処理端末１００に配布する。

尚、サーバ装置１２０ａが情報処理端末１００に再度配布をしないのは、プログラム固有情報のみであり、プログラムの本体は２回以上配布しても構わない。これは、プログラム固有情報がＣＲＬ８００により無効化されているため、プログラム固有情報が更新されない限り、不正使用を図る情報処理端末１００のユーザが新たなアプリケーションデータを取得することを排除しているためである。

図９は、本実施の形態１に係るプログラムヘッダ９００とプログラム９１０に含まれる別のデータ構造を示す図である。図９において、図３と異なる点は、プログラム９１０にＣＡ署名３１１を付加しない点である。

プログラムヘッダ９００は、プログラム９１０に関する情報を格納す

るものであり、上述したプログラムヘッダ３００と同様の情報であるプログラムＩＤ（９０１）、バージョン番号（９０２）、プログラムサイズ（９０３）、ハッシュ値（９０４）、ＣＡ署名（９０５）を含むものである。

プログラムヘッダ９００及びプログラム９１０の正当性検証を情報処理端末１００において行う場合、第１に、プログラムヘッダ９００をサーバ装置１２０から取得し、プログラムヘッダ９００に付加されたＣＡ署名９０５を検証する。これにより、情報処理端末１００はプログラムヘッダ９００が改ざんされていない、正当な配布元から配布された情報であることを検証する。

次に、プログラム９１０のハッシュ値を算出する。算出したハッシュ値と、プログラムヘッダ９００に格納されているプログラムのハッシュ値９０４を比較し、一致することを確認する。これにより、情報処理端末１２０はプログラム９１０が改ざんされていない正当な配布元から配布された情報であることを検証することが可能となる。

このように、プログラム９１０の正当性検証にプログラムヘッダ９００に格納されたプログラムのハッシュ値９０４を使用し、プログラムヘッダ９００にのみＣＡ署名９０５を付加することで、プログラム９１０のＣＡ署名に必要とする情報を低減しながら、プログラムヘッダ９００、プログラム９１０に署名を付加する場合と同様に正当性を検証することが可能となる。また、プログラムヘッダ９００とプログラム９１０の組み合わせが不正に変更された場合、情報処理端末１００において、プログラムのハッシュ値を算出することにより組み合わせの異常を検出することが可能となる。尚、プログラム９１０のＣＡ署名を行わないことにより、プログラム９１０を認証局に渡してＣＡ署名を行う必要がなくなる。

次に、図１０を用いて、固有情報ヘッダ１０００とプログラム固有情報１０２０とに含まれる別のデータ構造を示す図である。図１０において、図４と異なる点は、固有情報ヘッダ１０００がプログラム固有情報ハッシュ値１００５を有し、プログラム固有情報１０２０にＣＡ署名４２２を付加しない点である。

固有情報ヘッダ１０００は、プログラム固有情報１０２０に関する情報を格納するものであり、上述した固有情報ヘッダ４００に格納される情報と同様な情報であるプログラム固有情報ＩＤ１００１、プログラムＩＤ１００２、固有情報の数１００３、プログラム固有情報全体のサイズ１００４、プログラム固有情報全体のハッシュ値１００５、固有情報サブヘッダ１００６、及び固有情報ヘッダ全体に対するＣＡ署名１００７より構成される。

従って、情報処理端末１００は、プログラム固有情報１０２０のハッシュ値を算出して、算出したハッシュ値と、固有情報ヘッダ１０００に格納されているプログラム固有情報のハッシュ値１００５とを比較して一致することを確認することにより、プログラム固有情報１０２０が改ざんされていない、正当な配布元から配布された情報であることを検証することが可能となる。

以上のように、本実施の形態１に係るサーバ装置１２０が固有情報配布履歴保持部１４０を有することにより、サーバ装置１２０は、情報処理端末１００が以前に配布したプログラムに対応するプログラム固有情報の新規取得を防止することが可能となる。このため、新たなプログラム固有情報４２０を取得して排除の回避を図る情報処理端末１００のハッキング等の不正行為を回避してセキュアなダウンロードを実現できる。

また、情報処理端末１００においてサーバ装置１２０から取得したプログラムを内部からのみアクセス可能なセキュアなフラッシュメモリ等

に記録されている端末固有鍵１１０で暗号化することにより、従来のようにサーバ装置においてプログラムを情報処理端末の固有の鍵で暗号化する処理を必要としなくなり、サーバ装置１２０におけるプログラム暗号化処理の負担を軽減することが可能となる。尚、この場合、情報処理端末１００において端末固有鍵１１０で暗号化した場合、正しく暗号化が行えたことを確認する必要がある。この点に関し本発明では、情報処理端末１００は、プログラム格納後に端末固有鍵１１０で復号し、平文プログラムのハッシュ値による検証を行うことで、情報処理端末１００毎に異なる端末固有鍵１１０による暗号化を意識することなく、プログラム格納の成否を判定することが可能となる。

さらに、サーバ装置１２０は、プログラム全体をプログラム３１０及びプログラム固有情報４２０に分離して個別に作成している。従って、サーバ装置１２０は、各情報処理端末１００で異なる情報となる容量の比較的小さなプログラム固有情報４２０を複数管理して、全情報処理端末１００で共通な情報となる容量の大きなプログラム３１０は１つのみ管理することにより、サーバ装置１２０で管理する配布情報の容量を格段に低減され、ひいては、情報管理の負担を軽減することが可能となる。

そして、サーバ装置１２０においては、固有情報ヘッダ１０００にプログラム固有情報１０２０のハッシュ値１００５を格納し、固有情報ヘッダ１０００にのみＣＡ署名１００７を付加することで、プログラム９１０のＣＡ署名に必要とする情報を低減しながら、固有情報ヘッダ１０００、プログラム固有情報１０２０に署名を付加する場合と同様の効果を得ることが可能となる。また、固有情報ヘッダ１０００とプログラム固有情報１０２０の組み合わせが不正に変更された場合、情報処理端末１００において、プログラム固有情報１０２０のハッシュ値を算出することにより組み合わせの異常を検出することが可能となる。

尚、本実施の形態１で示した固有情報配布履歴保持部１４０に保持される固有情報配布履歴６００の形式は一例であり、最終配布日付６０３を削除してもよいし、他の情報を付加してもよい。また、本実施の形態１では固有情報配布履歴６００に記載されている端末ＩＤ６０１に対してプログラム固有情報４２０の配布を拒否しているが、不正取得でない限りにおいては、当該端末ＩＤ６０１を有する情報処理端末１００に対して既に配布済みのプログラム固有情報４２０を再度配布してもよい。

そして、本実施の形態１に係るサーバ装置１２０では、情報処理端末１００からの要求はプログラムの配布を伴うプログラム配布要求、又はプログラムの配布を伴わないプログラム固有情報配布要求のいずれかとできる。

また、本実施の形態１では情報処理端末１００とサーバ装置１２０間でＳＳＬを用いた暗号化データの送受信を行っているが、２点間で安全にデータの送受信が行える方法であれば、ＳＳＬに限らず他のプロトコルを用いてもよい。

そして、本実施の形態１ではデータ格納部１０６とプログラム格納部１０５を別にしているが、同一の格納部としてもよい。また、秘匿情報格納部１０７に端末公開鍵証明書１１３を格納しているが、データ格納部１０６に格納してもよい。

また、本実施の形態１に係るサーバ装置１２０は、プログラムヘッダ３００、固有情報ヘッダ４００をプログラム３１０、プログラム固有情報４２０とは別に作成しているが、プログラム３１０とプログラムヘッダ３００、プログラム固有情報４２０と固有情報ヘッダ４００をそれぞれ一体の情報とし、サーバ装置１２０からの配布に先立ちヘッダ部分のみ切り出して情報処理端末１００に送信してもよい。

さらに、本実施の形態１ではプログラム３１０、プログラム固有情報

４２０に対し配布時にセッション鍵による暗号化を行う例を示したが、セッション鍵とは異なる鍵でさらに暗号化し、その鍵をプログラムヘッダ３００、固有情報ヘッダ４００に含めて配布する構成としてもよい。

そして、本実施の形態１でハッシュ値と記載している点は、ハッシュアルゴリズムとしてＳＨＡ－１、ＭＤ５などの既存のハッシュアルゴリズムを使用してもよいし、独自のアルゴリズムを用いてもよい。また、ハッシュアルゴリズムのかわりにチェックサムなどの方法を用いて改ざんの検出を行ってもよい。また、情報処理端末１００毎に異なる情報を必要としないプログラムを配布する場合は、プログラム固有情報の配布を行う必要はない。

（実施の形態２）

図１１は、本発明の実施の形態２に係る情報処理端末１１００とサーバ装置１１２０との構成図を示す。同図において、実施の形態１と異なる点は、サーバ装置１１２０がプログラム／固有情報対応表保持部１１５０を保持する点である。

このプログラム／固有情報対応表保持部１１５０は、プログラム固有情報を一意に識別するプログラム固有情報ＩＤと、プログラム固有情報を使用するプログラムを一意に特定するプログラムＩＤとの対応を示したプログラム／固有情報対応表１２１０を保持する記憶部である。

図１２（ａ）及び（ｂ）は、本実施の形態２に係る固有情報配布履歴１２００及びプログラム／固有情報対応表１２１０に含まれる情報の一例を示す図である。

固有情報配布履歴保持部１１４０は、前述した実施の形態１の固有情報配布履歴６００と異なり、配布したプログラム固有情報に対応するプログラムを識別するプログラムＩＤ１２０２が付加されている固有情報配布履歴１２００を管理する。尚、固有情報配布履歴１２００に格納さ

れる端末ＩＤ１２０１、プログラム固有情報ＩＤ１２０３、及び最終配布日付１２０４については前述した図６と同様のため詳細な説明は省略する。

固有情報配布履歴１２００の例では、サーバ装置１１２０は情報処理端末１１００に５つのプログラム固有情報ＩＤ１２０３を配布済みであり、それぞれの端末ＩＤ１２０１、プログラムＩＤ１２０２、プログラム固有情報ＩＤ１２０３の組は、（端末ＩＤ，プログラムＩＤ，プログラム固有情報ＩＤ）＝（０００１，０００１，０００１）、（０００２，０００１，０００２）、（００１０，０００１，０００３）、（００１５，０００１，０００４）、（００２０，０００２，１００１）となる。

また、プログラム／固有情報対応表保持部１１５０は、プログラム／固有情報対応表１２１０に、サーバ装置１１２０が管理しているプログラムのプログラムＩＤ１２１１と、各プログラムが使用するプログラム固有情報を識別するプログラム固有情報ＩＤ１２１２との対応関係を格納する。

図１２の例では、サーバ装置１１２０はプログラムＩＤが０００１のプログラムを管理しており、そのプログラムが使用するプログラム固有情報としてプログラム固有情報ＩＤが０００１から１０００までのプログラム固有情報を管理している。同様にプログラムＩＤが０００２のプログラムと、そのプログラムが使用するプログラム固有情報ＩＤが１００１から２０００までのプログラム固有情報を管理している。また、プログラム／固有情報対応表１２１０には、情報処理端末１１００に配布済みのプログラム固有情報の再配布を防止するために、次回のプログラム固有情報配布の開始時に、配布すべきプログラム固有情報である配布開始ＩＤ１２１３を格納する。

図１２の例では、プログラムＩＤが０００１のプログラムに対し新た

にプログラム固有情報を割り当てる場合、サーバ装置１１２０はプログラム固有情報ＩＤ０１２３のプログラム固有情報を割り当てることを示している。同様にプログラムＩＤが０００２のプログラムに対し新たにプログラム固有情報を割り当てる場合、サーバ装置１１２０はプログラム固有情報ＩＤ１４２３のプログラム固有情報を割り当てることを示している。

また、サーバ装置１１２０は、このプログラム／固有情報対応表１２１０を用いて、情報処理端末１１００からのプログラムＩＤを指定したプログラム配布要求に対し、そのプログラムＩＤに対応したプログラム固有情報を配布することとなる。

本発明の実施の形態２におけるプログラム配布手順について、図１３を用いて説明する。図１３は、サーバ装置１１２０におけるプログラムの配布手順を示すフローチャートである。

第１に、サーバ装置１１２０は情報処理端末１１００からプログラム配布要求を受信する（Ｓ１３０１）。このプログラム配布要求は、プログラムＩＤを指定するものである。

次に、サーバ装置１１２０は、受信したプログラム配布要求から情報処理端末１１００の端末ＩＤ及びプログラムＩＤを取得する（Ｓ１３０２）。そして、固有情報配布履歴１２００に対して取得した端末ＩＤ、プログラムＩＤを検索し（Ｓ１３０３）、固有情報配布履歴１２００に同じ端末ＩＤかつ同じプログラムＩＤの履歴が格納されているか否か確認する（Ｓ１３０４）。

固有情報配布履歴１２００に同じ端末ＩＤかつ同じプログラムＩＤの履歴が格納されていた場合には（Ｓ１３０４でＹ）、サーバ装置１１２０は、情報処理端末１１００に既に指定プログラムに対するプログラム固有情報１１３５を配布済みであるため、プログラム１１３３のみを送

信し処理を終了する（Ｓ１３０９）。

固有情報配布履歴１２００に同じ端末ＩＤかつ同じプログラムＩＤの履歴が格納されていない場合には（Ｓ１３０４でＮ）、サーバ装置１１２０は、プログラム／固有情報対応表１２１０に格納されている配布開始ＩＤの情報を元に情報処理端末１１００へ新たにプログラム固有情報１１３５を割り当てる（Ｓ１３０５）。

次に、サーバ装置１１２０は、新たに割り当てたプログラム固有情報１１３５に関し、プログラム／固有情報対応表保持部１１５０に格納されているプログラム／固有情報対応表１２１０を参照して、配布開始ＩＤ１２１３の値を更新する（Ｓ１３０６）。また、新たに割り当てたプログラム固有情報１１３５に関し、端末ＩＤとプログラム固有情報ＩＤの対応を固有情報配布履歴１２００に追加する（Ｓ１３０７）。そして、サーバ装置１１２０は、プログラム固有情報１１３５を情報処理端末１１００に送信し（Ｓ１３０８）、プログラム１１３３を送信し処理を終了する（Ｓ１３０９）。

以上のように、本実施の形態２に係るサーバ装置１１２０は、固有情報配布履歴保持部１１４０とプログラム／固有情報対応表保持部１１５０とを有し、固有情報配布履歴１２００とプログラム／固有情報対応表１２１０を用いてプログラム固有情報の配布管理を行うことにより、１つの情報処理端末１１００で動作する同一プログラムに対して複数のプログラム固有情報１１３５を配布することを防ぐ。このため、新たなプログラム固有情報１１３５を取得して排除の回避を図る情報処理端末１１００がプログラム固有情報１１３５を新規取得することを防止することが可能となる。

また、本実施の形態２に係るサーバ装置１１２０は、ダウンロード対象のプログラムと、当該プログラムが動作する情報処理端末１１００と

の対応をプログラム／固有情報対応表１２１０に格納してプログラム固有情報１１３５の配布をプログラム単位に管理することにより、プログラム毎にプログラム固有情報１１３５の配布可否を判定することが可能となる。このため、サーバ装置１１２０はプログラム／固有情報対応表１２１０を参照して、プログラムを動作対象でない情報処理端末１１００に配布することを防止することが可能となる。

尚、本実施の形態２ではデータ格納部１１０６とプログラム格納部１１０５を別にしているが、同一の格納部としてもよい。また、本実施の形態２で示した固有情報配布履歴１２００の形式は一例であり、最終配布日付１２０４を削除してもよいし、他の情報を付加してもよい。同様にプログラム／固有情報対応表１２１０の形式も一例であり、配布開始ＩＤ１２１３を別の形式で管理してもよい。例えば、全プログラム固有情報ＩＤを格納したテーブルを持ち、各プログラム固有情報ＩＤに対して割り当て済みか否かを識別するフラグを設けることにより、プログラム固有情報１１３５の配布状態を管理してもよい。

また、本実施の形態２では固有情報配布履歴１２００に記載されている端末ＩＤ１２０１に対してプログラム固有情報１１３５の配布を拒否しているが、その情報処理端末１１００に対して既に配布済みのプログラム固有情報１１３５を再度配布してもよい。また、本実施の形態２では情報処理端末１１００からの要求はプログラムの配布を伴うプログラム配布要求、又はプログラムの配布が伴わないプログラム固有情報配布要求とできる。

（実施の形態３）

図１４は、本実施の形態３に係る情報処理端末１４００とサーバ装置１４２０の構成図を示す。同図において、前述した実施の形態１及び実施の形態２と異なる点は、サーバ装置１４２０が配布回数情報保持部１

４４０を有する点である。

この配布回数情報保持部１４４０は、サーバ装置１４２０から同一の情報処理端末１４００に対してプログラム固有情報１４３５を配布した回数を管理するための配布回数情報１５００を保持するハードディスクである。

図１５は、本実施の形態３に係る配布回数情報１５００の情報格納例を示す図である。

配布回数情報１５００には、プログラム固有情報１４３５を配布した情報処理端末１４００を識別するＩＤである端末ＩＤ１５０１、配布した回数を示す回数カウンタ１５０２が格納される。同図の例では、端末ＩＤが０００１、０００２の情報処理端末１４００に対してプログラム固有情報１４３５を１回配布しており、端末ＩＤが０００３の情報処理端末１４００に対してプログラム固有情報１４３５を配布していないことが示されている。

図１６は、サーバ装置１４２０におけるプログラムの配布手順を示すフローチャートである。

まず、サーバ装置１４２０は情報処理端末１４００からプログラム配布要求を受信する（Ｓ１６０１）。次に、サーバ装置１４２０は、Ｓ１６０１で受信したプログラム配布要求に含まれる情報処理端末１４００の端末ＩＤを取得する（Ｓ１６０２）。

そして、サーバ装置１４２０は配布回数情報保持部１４４０に保持される配布回数情報１５００を用いてＳ１６０２で取得した端末ＩＤを検索し、回数カウンタの値を取得する（Ｓ１６０３）。また、取得した回数カウンタの値が規定値以上か否かを判定する（Ｓ１６０４）。

そして、取得した回数カウンタの値が規定値以上であった場合（Ｓ１６０４でＹ）、サーバ装置１４２０は、情報処理端末１４００に対して

は既にプログラム固有情報１４３５を規定回数以上配布しているため、プログラム１４３３のみを送信し処理を終了する（Ｓ１６０８）。

一方、取得した回数カウンタの値が規定値未満であった場合（Ｓ１６０４でＮ）、サーバ装置１４２０は情報処理端末１４００へは新たにプログラム固有情報１４３５を割り当てる（Ｓ１６０５）。また、サーバ装置１４２０は配布回数情報保持部１４４０内に格納されている配布回数情報１５００の回数カウンタの値を加算する（Ｓ１６０６）。そして、サーバ装置１４２０は、プログラム固有情報１４３５を情報処理端末１４００に送信し（Ｓ１６０７）、プログラム１４３３を送信し処理を終了する（Ｓ１６０８）。

このように、本実施の形態３に係るサーバ装置１４２０は、配布回数情報保持部１４４０を有し、配布回数情報１５００を用いてプログラム固有情報１４３５の配布管理を行うことにより、１つの情報処理端末１４００へ規定値以上のプログラム固有情報１４３５を配布することを防ぐことができる。特に、規定値を１に設定した場合、本発明の実施の形態１及び実施の形態２と同様に、サーバ装置１４２０は、プログラム固有情報１４３５が含む情報を用いて不正端末と認識され、排除されている情報処理端末１４００に対し、新たにプログラム固有情報１４３５を割り当てることにより、不正端末が排除を回避することを防ぐことが可能となる。

また、プログラム固有情報１４３５の配布回数を示す規定値を２以上とすることにより、ハードディスクが故障したような不正の目的でなくプログラムを再度購入するようなユーザに対してプログラム固有情報１４３５の再配布や新たな配布を正規に行うことが可能となる。

尚、本実施の形態３ではデータ格納部１４０６とプログラム格納部１４０５を別にしているが、同一の格納部としてもよい。また、本実施の

形態３で示した配布回数情報１５００の形式は一例であり、他の情報を付加してもよい。また、本実施の形態３では情報処理端末１４００からの要求はプログラムの配布を伴うプログラム配布要求、又はプログラムの配布要求を伴わないプログラム固有情報配布要求とできる。

（実施の形態４）

図１７は、本実施の形態４に係る情報処理端末１７００とサーバ装置１７２０の構成図を示す。同図において、前述の実施の形態３と異なる点は、サーバ装置１７２０がプログラム／固有情報対応表保持部１７５０を保持する点である。このプログラム／固有情報対応表保持部１７５０は、図１１において説明したプログラム／固有情報対応表保持部１１５０と同様の記憶部である。

図１８（ａ）及び（ｂ）は、本実施の形態４に係る配布回数情報１８００とプログラム／固有情報対応表１８１０に格納されるデータの一例を示す図である。

配布回数情報１８００は、配布したプログラムのプログラムＩＤ１８０１、プログラム固有情報１７３５を配布した情報処理端末１７００の端末ＩＤ１８０２、プログラム固有情報を配布した回数を示す回数カウンタ１８０３を格納する。前記実施の形態３における配布回数情報１５００と異なる点は、プログラム固有情報を使用するプログラムを識別するプログラムＩＤ１８０１が付加されている点である。

配布回数情報１８００は、プログラムＩＤが０００１のプログラムが使用するプログラム固有情報１７３５を、端末ＩＤが０００１、０００２の情報処理端末１７００に対して１回配布し、端末ＩＤが０００３の情報処理端末１７００に対してプログラム固有情報１７３５を配布していないことを示す。また同様に、プログラムＩＤが０００２のプログラムが使用するプログラム固有情報１７３５を、端末ＩＤが０００１の情

報処理端末１７００に対して１回配布しており、端末ＩＤが０００２、０００３の情報処理端末１７００に対してプログラム固有情報１７３５を配布していないことを示している。

尚、プログラム／固有情報対応表１８１０は、前述した図１２におけるプログラム／固有情報対応表１２１０と同様であり、詳細な説明は省略する。

図１９は、サーバ装置１７２０におけるプログラムの配布手順を示すフローチャートである。

まず、サーバ装置１７２０は情報処理端末１７００からプログラム配布要求を受信する（Ｓ１９０１）。このプログラム配布要求には、情報処理端末１７００より取得の要求されるプログラムのプログラムＩＤを含む。次に、サーバ装置１７２０は、Ｓ１９０１で受信したプログラム配布要求に含まれる情報処理端末１７００の端末ＩＤ、プログラムＩＤを取得する（Ｓ１９０２）。

そして、サーバ装置１７２０は、配布回数情報１８００に対してＳ１９０２で取得した端末ＩＤ、プログラムＩＤを検索し、回数カウンタの値を取得する（Ｓ１９０３）。次に、取得した回数カウンタの値が規定値以上か否かを判定する（Ｓ１９０４）。

また、取得した回数カウンタの値が規定値以上であった場合（Ｓ１９０４でＹ）、サーバ装置１７２０は、情報処理端末１７００へは既にプログラム固有情報１７３５を規定回数以上配布しているため、プログラム１７３３のみを送信し処理を終了する（Ｓ１９０９）。

次に、取得した回数カウンタの値が規定値未満であった場合（Ｓ１９０４でＮ）、サーバ装置１７２０は、プログラム／固有情報対応表１８１０に格納されている配布開始ＩＤの情報を元に情報処理端末１７００へ新たにプログラム固有情報１７３５を割り当てる（Ｓ１９０５）。

そして、サーバ装置１７２０は、Ｓ１９０５で新たに割り当てたプログラム固有情報１７３５に関し、プログラム／固有情報対応表１８１０に格納されている配布開始ＩＤの値を更新する（Ｓ１９０６）。また、配布回数情報１８００内に格納されている回数カウンタの値を加算し（Ｓ１９０７）、プログラム固有情報１７３５を情報処理端末１７００に送信し（Ｓ１９０８）、プログラム１７３３を送信し処理を終了する（Ｓ１９０９）。

以上のように、本実施の形態４に係るサーバ装置１７２０は、配布回数情報保持部１７４０とプログラム／固有情報対応表保持部１７５０とを有し、各保持部に保持される配布回数情報１８００及びプログラム／固有情報対応表１８１０を用いてプログラム固有情報１７３５を配布管理することにより、１つの情報処理端末１７００で動作する同一プログラムに対して規定値以上のプログラム固有情報１７３５を配布することを防いで、プログラム固有情報１７３５の不正使用を図る情報処理端末１７００を排除することが可能となる。

また、本実施の形態４では、サーバ装置１７２０は、プログラム固有情報の配布をプログラム単位に管理することにより、プログラム毎にプログラム固有情報１７３５の配布可否を判定することが可能となる。

尚、本実施の形態４ではデータ格納部１７０６とプログラム格納部１７０５を別にしているが、同一の格納部としてもよい。また、本実施の形態４で示した配布回数情報１８００の形式は一例であり、他の情報を付加してもよい。同様にプログラム／固有情報対応表１８１０の形式も一例であり、別の形式で管理してもよい。また、本実施の形態４では情報処理端末１７００からの要求はプログラムの配布を伴うプログラム配布要求、又はプログラムの配布を伴わないプログラム固有情報配布要求とできる。

以上のように、本発明に係るサーバ装置は、固有情報配布履歴保持部を有することにより、情報処理端末が以前に配布したプログラムに対応するプログラム固有情報の新規取得を防止することが可能となり、新たなプログラム固有情報を取得して排除の回避を図る情報処理端末の不正行為を確実に防止することが可能となる。

また、本発明に係る情報処理端末は、サーバ装置から取得したプログラムを端末固有鍵で暗号化することにより、サーバ装置におけるプログラム暗号化処理の負担を軽減することが可能となる。さらに、本発明に係るサーバ装置は、プログラム全体をプログラム及びプログラム固有情報に分離して個別に作成しているため、サーバ装置は、各情報処理端末で異なる情報となる容量の比較的小さなプログラム固有情報を複数管理して、全情報処理端末で共通な情報となる容量の大きなプログラムは1つのみ管理して、サーバ装置で管理する配布情報の容量を低減することが可能となり、情報管理の負担を軽減することが可能となる。

そして、本発明に係るサーバ装置から情報処理端末に配布されるプログラムの全体には、情報処理端末で動作するプログラム本体、プログラムヘッダ、プログラム固有情報、及び固有情報ヘッダが含まれるため、プログラムを構成する各情報にＣＡ署名やハッシュ値を用いることにより、サーバ装置から情報処理端末に配布される情報の正当性を確認することが可能となる。

産業上の利用の可能性

本発明に係るサーバ装置及びプログラム管理システムは、通信機能を備えるパーソナルコンピュータ、携帯電話等の情報処理端末にネットワークを介してプログラムを配布するサーバ装置、及び当該サーバ装置と情報処理端末との間のプログラム管理システムとして有用である。

請　求　の　範　囲

1．　外部から書き換えが行えない端末ＩＤを保持する情報処理端末とネットワークを介して接続され前記情報処理端末で動作するプログラムを保持するサーバ装置であって、

以前に配布したプログラムと端末ＩＤとの関連を示すテーブルを保持するテーブル保持手段と、

前記テーブルを参照して、前記情報処理端末から送信され前記端末ＩＤを伴うプログラム取得要求に対するプログラムの配布をするか否かを判定する判定手段とを備える

ことを特徴とするサーバ装置。

2．　前記プログラムには、前記情報処理端末で動作するプログラム本体、及び当該プログラム本体に使用される固有の情報であるプログラム固有情報が含まれ、

前記判定手段は、

前記プログラム取得要求に付与されている前記端末ＩＤが前記テーブルに記録されている場合には、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、

前記端末ＩＤが前記テーブルに記載されていない場合には、前記端末ＩＤと前記プログラム固有情報とを対応させて前記テーブルに追加すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する

ことを特徴とする請求項１記載のサーバ装置。

3．　前記判定手段は、

前記情報処理端末からの前記プログラム取得要求に対して、前記プログラム本体の配布は前記プログラム取得要求毎に行うと判定する一方、

前記プログラム固有情報の配布は１回のみ行うと判定する

ことを特徴とする請求項２記載のサーバ装置。

４．　前記テーブル保持手段は、

前記端末ＩＤと前記プログラム固有情報の配布回数とを示すテーブルを保持し、

前記判定手段は、

前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末ＩＤに対応する配布回数が規定値に達している場合においては、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、

前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末ＩＤに対応する配布回数が規定値に達していない場合においては、前記端末ＩＤに対応させて前記テーブルに記載されている配布回数を更新すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する

ことを特徴とする請求項１記載のサーバ装置。

５．　前記テーブル保持手段は、

前記情報処理端末からのプログラム取得要求に付与されている前記端末ＩＤと、前記端末ＩＤの情報処理端末に配布した前記プログラム本体を一意に特定するプログラム本体ＩＤと、前記端末ＩＤの情報処理端末にプログラム固有情報を配布した回数を示す配布回数との関連を示すテーブルを保持し、

前記判定手段は、

前記テーブルを参照して、前記情報処理端末より配布された前記プロ

グラム取得要求に付与されている前記端末ＩＤと前記プログラムＩＤとの両方に対応する配布回数が規定値に達している場合においては、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、

前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末ＩＤ及び前記プログラムＩＤに対応する配布回数が規定値に達していない場合においては、前記端末ＩＤと前記プログラムＩＤとに対応させて前記テーブルに記載されている配布回数を更新すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する

ことを特徴とする請求項４記載のサーバ装置。

６．　前記規定値は、前記サーバ装置から前記情報処理端末に配布するプログラム固有情報の配布回数を示す値である

ことを特徴とする請求項４又は請求項５記載のサーバ装置。

７．　前記テーブル保持手段は、

前記情報処理端末からのプログラム取得要求に付与されている前記端末ＩＤと、前記端末ＩＤの情報処理端末に配布した前記プログラム本体を一意に特定するプログラム本体ＩＤと、前記端末ＩＤの情報処理端末に配布したプログラム固有情報を一意に特定するプログラム固有情報ＩＤとの関連を示すテーブルを保持し、

前記判定手段は、

前記テーブルを参照して、前記情報処理端末より送信された前記プログラム取得要求に付与されている前記端末ＩＤと前記プログラムＩＤとの両方に対応するプログラム固有情報ＩＤが記載されている場合においては、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、

前記テーブルを参照して、前記プログラム取得要求に付与されている前記端末ＩＤと前記プログラムＩＤとの両方に対応するプログラム固有情報ＩＤが記載されていない場合においては、前記端末ＩＤと前記プログラム固有情報ＩＤと前記プログラムＩＤとを対応させて前記テーブルに追加すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する

ことを特徴とする請求項１記載のサーバ装置。

８．　前記サーバ装置は、

前記情報処理端末毎に異なる情報となる前記プログラム固有情報を複数保持し、

前記情報処理端末で共通な前記プログラム本体を１つ保持する

ことを特徴とする請求項２記載のサーバ装置。

９．　前記テーブル保持手段は、

前記プログラム本体を一意に特定するプログラム本体ＩＤと、前記プログラム本体が動作する前記情報処理端末の端末ＩＤとの関連を示すテーブルを保持し、

前記判定手段は、

前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末ＩＤと前記プログラムＩＤとが対応して記載されている場合においては、前記プログラムの配布可能と判定し、

前記テーブルを参照して、前記プログラム取得要求に付与されている前記端末ＩＤと前記プログラムＩＤとが対応して記載されていない場合においては、前記プログラム本体の配布不可と判定する

ことを特徴とする請求項２記載のサーバ装置。

１０．　外部から書き換えが行えない端末ＩＤを保持する情報処理端末

と、当該情報処理端末とネットワークを介して接続され前記情報処理端末で動作するプログラムを保持するサーバ装置とから構成されるプログラム管理システムであって、

前記情報処理端末は、

前記プログラムの取得を要求する場合には、前記端末ＩＤを付与したプログラム取得要求を前記サーバ装置に送信し、

前記サーバ装置は、

前記プログラム取得要求を受信して、以前に配布したプログラムと端末ＩＤとの関連を示すテーブルを保持するテーブル保持手段と、

前記テーブルを参照して、前記情報処理端末から送信されて前記端末ＩＤが付与されているプログラム取得要求に対するプログラムの配布をするか否かを判定する判定手段とを備える

ことを特徴とするプログラム管理システム。

１１．　前記情報処理端末は、外部から書き換えが行えないメモリ部に前記情報処理端末毎に異なる固有鍵を格納し、

前記サーバ装置から取得した前記プログラムを、前記固有鍵を用いて暗号化して前記情報処理端末内のメモリ部に格納する格納手段を備える

ことを特徴とする請求項１０記載のプログラム管理システム。

１２．　前記プログラムには、前記情報処理端末で動作するプログラム本体、当該プログラム本体に関する情報を格納するプログラムヘッダ、前記プログラム本体に使用される固有の情報であるプログラム固有情報、及び当該プログラム固有情報に関する情報を格納した固有情報ヘッダが含まれ、

前記情報処理端末は、

前記サーバ装置に取得を要求するプログラムに含まれる前記プログラムヘッダ及び前記固有情報ヘッダの取得を要求するヘッダ取得要求を行

い、

前記サーバ装置は、

前記判定手段において前記プログラム本体の配布可能と判定される場合においては、前記プログラムヘッダ及び前記固有情報ヘッダを前記情報処理端末に配布し、

前記情報処理端末は、

前記プログラムヘッダ及び前記固有情報ヘッダに基づいて検証を行う検証手段を備え、当該検証手段での検証を行った後に前記プログラム取得要求を前記サーバ装置に送信する

ことを特徴とする請求項１０記載のプログラム管理システム。

１３．　前記プログラムヘッダには、前記プログラムを一意に特定することが可能な認証子が含まれ、

前記情報処理端末は、前記固有鍵で暗号化され前記情報処理端末内のメモリ部に格納されているプログラムを前記固有鍵で復号し、前記認証子を用いて前記固有鍵での暗号化が正しく行われたことを検証する検証手段を備える

ことを特徴とする請求項１２記載のプログラム管理システム。

１４．　前記プログラム、前記プログラムヘッダ、前記プログラム固有情報、及び前記固有情報ヘッダには電子的な署名が付加されている

ことを特徴とする請求項１２記載のプログラム管理システム。

１５．　前記プログラムヘッダには、前記プログラムを一意に特定することが可能な認証子が含まれ、前記固有情報ヘッダには、前記プログラム固有情報を一意に特定することが可能な認証子が含まれる

ことを特徴とする請求項１２記載のプログラム管理システム。

１６．　外部から書き換えが行えない端末ＩＤを保持する情報処理端末と、当該情報処理端末とネットワークを介して接続され前記情報処理端

末で動作するプログラムを保持するサーバ装置とから構成されるプログラム配布方法であって、

前記情報処理端末は、

前記プログラムの取得を要求する場合には、前記端末ＩＤを付与したプログラム取得要求を前記サーバ装置に送信するステップを有し、

前記サーバ装置は、

前記プログラム取得要求を受信して、以前に配布したプログラムと端末ＩＤとの関連を示すテーブルを保持するテーブル保持ステップと、

前記テーブルを参照して、前記情報処理端末から送信されて前記端末ＩＤが付与されているプログラム取得要求に対するプログラムの配布をするか否かを判定する判定ステップとを有する

ことを特徴とするプログラム配布方法。

１７．　外部から書き換えが行えない端末ＩＤを保持する情報処理端末とネットワークを介して接続され前記情報処理端末で動作する配布プログラムを保持するサーバ装置で用いられるプログラムであって、

以前に配布した配布プログラムと端末ＩＤとの関連を示すテーブルを保持するテーブル保持ステップと、

前記テーブルを参照して、前記情報処理端末から送信され前記端末ＩＤを伴うプログラム取得要求に対する配布プログラムの配布をするか否かを判定する判定ステップとをコンピュータに実行させる

ことを特徴とするプログラム。

補正書の請求の範囲

［２００３年１０月７日（０７．１０．０３）国際事務局受理：出願当初の請求の範囲１，１０，１６及び１７は取り下げられた；新しい請求の範囲１８及び１９が加えられた；他の請求の範囲は変更なし。（７頁）］

１．（削除）

２．（補正後）外部から書き換えが行えない端末ＩＤを保持する情報処理端末とネットワークを介して接続され、

以前に配布したプログラムと端末ＩＤとの関連を示すテーブルを参照して、前記情報処理端末から送信された前記端末ＩＤを伴うプログラム取得要求に対するプログラムの配布をするか否かを判定するサーバ装置であって、

前記プログラムには、前記情報処理端末で動作するプログラム本体、及び当該プログラム本体に使用される固有の情報であるプログラム固有情報が含まれ、

前記プログラム取得要求に付与されている前記端末ＩＤが前記テーブルに記録されている場合には、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、

前記端末ＩＤが前記テーブルに記載されていない場合には、前記端末ＩＤと前記プログラム固有情報とを対応させて前記テーブルに追加すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する判定手段を備える

ことを特徴とするサーバ装置。

３．　前記判定手段は、

前記情報処理端末からの前記プログラム取得要求に対して、前記プログラム本体の配布は前記プログラム取得要求毎に行うと判定する一方、前記プログラム固有情報の配布は１回のみ行うと判定する

ことを特徴とする請求項２記載のサーバ装置。

４．（補正後）前記テーブル保持手段は、

前記端末ＩＤと前記プログラム固有情報の配布回数とを示すテーブルを保持し、

前記判定手段は、

前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末ＩＤに対応する配布回数が規定値に達している場合においては、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、

前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末ＩＤに対応する配布回数が規定値に達していない場合においては、前記端末ＩＤに対応させて前記テーブルに記載されている配布回数を更新すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する

ことを特徴とする請求項２記載のサーバ装置。

５．　前記テーブル保持手段は、

前記情報処理端末からのプログラム取得要求に付与されている前記端末ＩＤと、前記端末ＩＤの情報処理端末に配布した前記プログラム本体を一意に特定するプログラム本体ＩＤと、前記端末ＩＤの情報処理端末にプログラム固有情報を配布した回数を示す配布回数との関連を示すテーブルを保持し、

前記判定手段は、

前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末ＩＤと前記プログラムＩＤとの両方に対応する配布回数が規定値に達している場合においては、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を

前記情報処理端末に行うと判定し、

前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末ＩＤ及び前記プログラムＩＤに対応する配布回数が規定値に達していない場合においては、前記端末ＩＤと前記プログラムＩＤとに対応させて前記テーブルに記載されている配布回数を更新すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する

ことを特徴とする請求項４記載のサーバ装置。

６．　前記規定値は、前記サーバ装置から前記情報処理端末に配布するプログラム固有情報の配布回数を示す値である

ことを特徴とする請求項４又は請求項５記載のサーバ装置。

７．（補正後）前記テーブル保持手段は、

前記情報処理端末からのプログラム取得要求に付与されている前記端末ＩＤと、前記端末ＩＤの情報処理端末に配布した前記プログラム本体を一意に特定するプログラム本体ＩＤと、前記端末ＩＤの情報処理端末に配布したプログラム固有情報を一意に特定するプログラム固有情報ＩＤとの関連を示すテーブルを保持し、

前記判定手段は、

前記テーブルを参照して、前記情報処理端末より送信された前記プログラム取得要求に付与されている前記端末ＩＤと前記プログラムＩＤとの両方に対応するプログラム固有情報ＩＤが記載されている場合においては、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、

前記テーブルを参照して、前記プログラム取得要求に付与されている前記端末ＩＤと前記プログラムＩＤとの両方に対応するプログラム固有情報ＩＤが記載されていない場合においては、前記端末ＩＤと前記プロ

グラム固有情報ＩＤと前記プログラムＩＤとを対応させて前記テーブルに追加すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する

ことを特徴とする請求項２記載のサーバ装置。

８．　前記サーバ装置は、

前記情報処理端末毎に異なる情報となる前記プログラム固有情報を複数保持し、

前記情報処理端末で共通な前記プログラム本体を１つ保持する

ことを特徴とする請求項２記載のサーバ装置。

９．　前記テーブル保持手段は、

前記プログラム本体を一意に特定するプログラム本体ＩＤと、前記プログラム本体が動作する前記情報処理端末の端末ＩＤとの関連を示すテーブルを保持し、

前記判定手段は、

前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末ＩＤと前記プログラムＩＤとが対応して記載されている場合においては、前記プログラムの配布可能と判定し、

前記テーブルを参照して、前記プログラム取得要求に付与されている前記端末ＩＤと前記プログラムＩＤとが対応して記載されていない場合においては、前記プログラム本体の配布不可と判定する

ことを特徴とする請求項２記載のサーバ装置。

１０．（削除）

１１．（補正後）外部から書き換えが行えない端末ＩＤを保持する情報処理端末と、

以前に配布したプログラムと端末ＩＤとの関連を示すテーブルを参照

して、前記情報処理端末から送信された前記端末ＩＤを伴うプログラム取得要求に対するプログラムの配布をするか否かを判定するサーバ装置とがネットワークを介して接続して構成されるプログラム管理システムであって、

前記情報処理端末は、外部から書き換えが行えないメモリ部に前記情報処理端末毎に異なる固有鍵を格納し、

前記サーバ装置から取得した前記プログラムを、前記固有鍵を用いて暗号化して前記情報処理端末内のメモリ部に格納する格納手段を備えることを特徴とするプログラム管理システム。

１２．（補正後）前記プログラムには、前記情報処理端末で動作するプログラム本体、当該プログラム本体に関する情報を格納するプログラムヘッダ、前記プログラム本体に使用される固有の情報であるプログラム固有情報、及び当該プログラム固有情報に関する情報を格納した固有情報ヘッダが含まれ、

前記情報処理端末は、

前記サーバ装置に取得を要求するプログラムに含まれる前記プログラムヘッダ及び前記固有情報ヘッダの取得を要求するヘッダ取得要求を行い、

前記サーバ装置は、

前記判定手段において前記プログラム本体の配布可能と判定される場合においては、前記プログラムヘッダ及び前記固有情報ヘッダを前記情報処理端末に配布し、

前記情報処理端末は、

前記プログラムヘッダ及び前記固有情報ヘッダに基づいて検証を行う検証手段を備え、当該検証手段での検証を行った後に前記プログラム取得要求を前記サーバ装置に送信する

ことを特徴とする請求項１１記載のプログラム管理システム。

１３．　前記プログラムヘッダには、前記プログラムを一意に特定することが可能な認証子が含まれ、

前記情報処理端末は、前記固有鍵で暗号化され前記情報処理端末内のメモリ部に格納されているプログラムを前記固有鍵で復号し、前記認証子を用いて前記固有鍵での暗号化が正しく行われたことを検証する検証手段を備える

ことを特徴とする請求項１２記載のプログラム管理システム。

１４．　前記プログラム、前記プログラムヘッダ、前記プログラム固有情報、及び前記固有情報ヘッダには電子的な署名が付加されている

ことを特徴とする請求項１２記載のプログラム管理システム。

１５．　前記プログラムヘッダには、前記プログラムを一意に特定することが可能な認証子が含まれ、前記固有情報ヘッダには、前記プログラム固有情報を一意に特定することが可能な認証子が含まれる

ことを特徴とする請求項１２記載のプログラム管理システム。

１６．（削除）

１７．（削除）

１８．（追加）外部から書き換えが行えない端末ＩＤを保持する情報処理端末とネットワークを介して接続され、

以前に配布したプログラムと端末ＩＤとの関連を示すテーブルを参照して、前記情報処理端末から送信された前記端末ＩＤを伴うプログラム取得要求に対するプログラムの配布をするか否かを判定するサーバ装置で用いられるプログラム配布方法であって、

前記プログラムには、前記情報処理端末で動作するプログラム本体、及び当該プログラム本体に使用される固有の情報であるプログラム固有情報が含まれ、

前記プログラム取得要求に付与されている前記端末ＩＤが前記テーブルに記録されている場合には、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、

前記端末ＩＤが前記テーブルに記載されていない場合には、前記端末ＩＤと前記プログラム固有情報とを対応させて前記テーブルに追加すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する判定ステップを含む

ことを特徴とするプログラム配布方法。

１９．（追加）外部から書き換えが行えない端末ＩＤを保持する情報処理端末とネットワークを介して接続され、

以前に配布したプログラムと端末ＩＤとの関連を示すテーブルを参照して、前記情報処理端末から送信された前記端末ＩＤを伴うプログラム取得要求に対するプログラムの配布をするか否かを判定するサーバ装置で用いられるプログラムであって、

前記プログラムには、前記情報処理端末で動作するプログラム本体、及び当該プログラム本体に使用される固有の情報であるプログラム固有情報が含まれ、

前記プログラム取得要求に付与されている前記端末ＩＤが前記テーブルに記録されている場合には、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、

前記端末ＩＤが前記テーブルに記載されていない場合には、前記端末ＩＤと前記プログラム固有情報とを対応させて前記テーブルに追加すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する判定ステップを含む

ことを特徴とするプログラム。

条約第１９条（１）に基づく説明書

請求の範囲第２項は、サーバ装置が保持するプログラムには、プログラム本体、プログラム固有情報が含まれることを明確にし、また、サーバ装置の判定手段は端末ＩＤを用いてプログラム固有情報の配布を管理することを明確にした。

請求の範囲第４項、７項は、従属先である第１項を削除したため、第２項に従属させた。

請求の範囲第１１項は、従属先である第１０項を削除したために、プリアンブル部を補足すると共に、独立クレームとした。

請求の範囲第１２項は、従属先である第１０項を削除したために、請求の範囲第１１項に従属させた。

請求の範囲第１項の削除に伴い、対応するプログラム配布方法及びプログラムである第１６項及び第１７項を削除した。また、新たに請求の範囲第２項に対応するプログラム配布方法及びプログラムに対応する請求の範囲第１８項及び第１９項を追加した。

出願人は、請求の範囲１、１０、１６、１７を削除し、請求の範囲２、４、７、１１、１２を補正し、請求の範囲３、５、６、８、９、１３、１４、１５は変更なく、新たに請求の範囲１８及び１９項を追加した。

図1

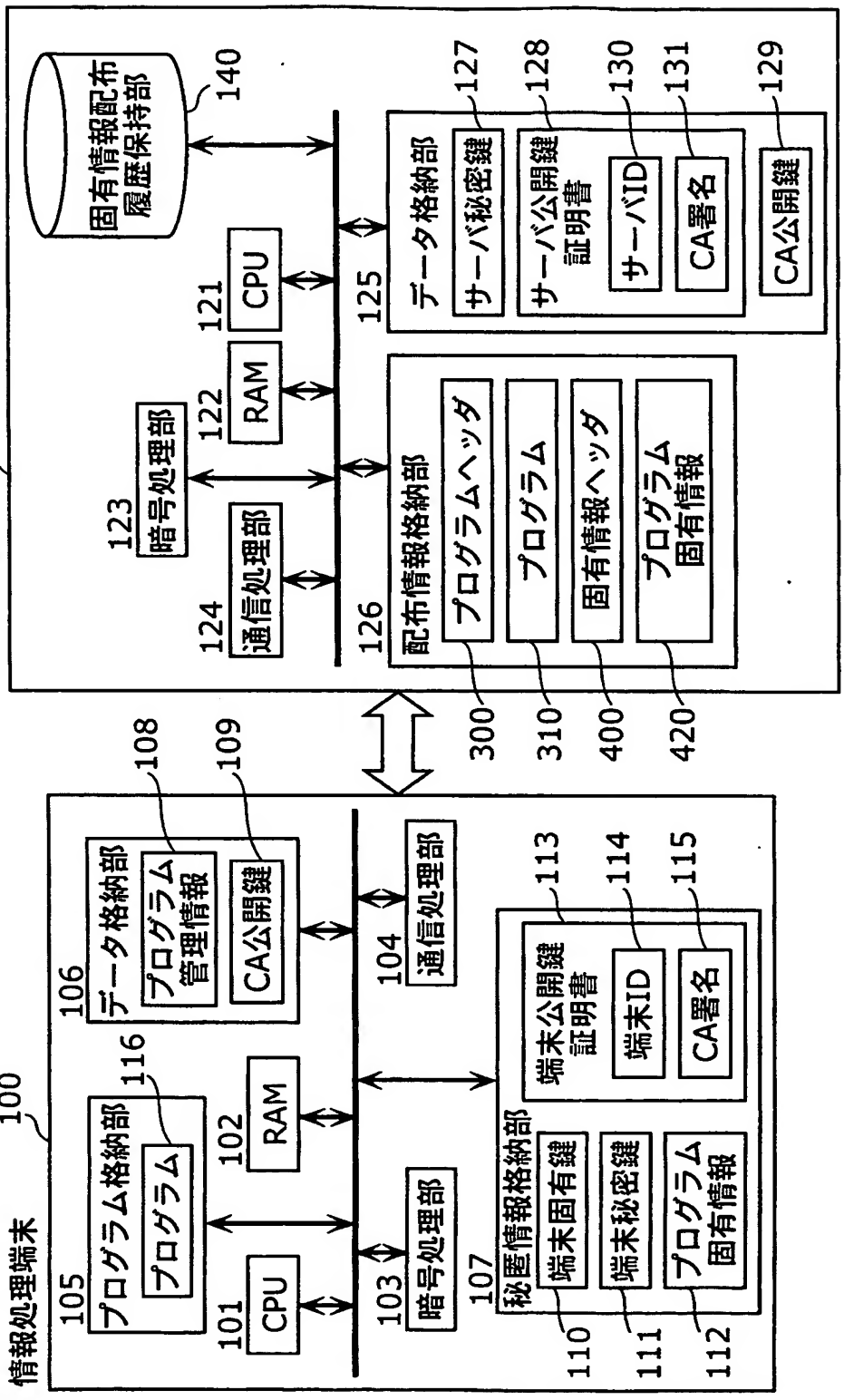

情報処理端末
100
CPU
101
RAM
102
暗号処理部
103
通信処理部
104
プログラム格納部
105
プログラム
116
データ格納部
106
プログラム管理情報
108
CA公開鍵
109
秘匿情報格納部
107
端末固有鍵
110
端末秘密鍵
111
プログラム固有情報
112
端末公開鍵証明書
113
端末ID
114
CA署名
115
サーバ装置
120
CPU
121
RAM
122
暗号処理部
123
通信処理部
124
配布情報格納部
126
プログラムヘッダ
300
プログラム
310
固有情報ヘッダ
400
プログラム固有情報
420
データ格納部
125
サーバ秘密鍵
127
サーバ公開鍵証明書
128
サーバID
130
CA署名
131
CA公開鍵
129
固有情報配布履歴保持部
140

図2

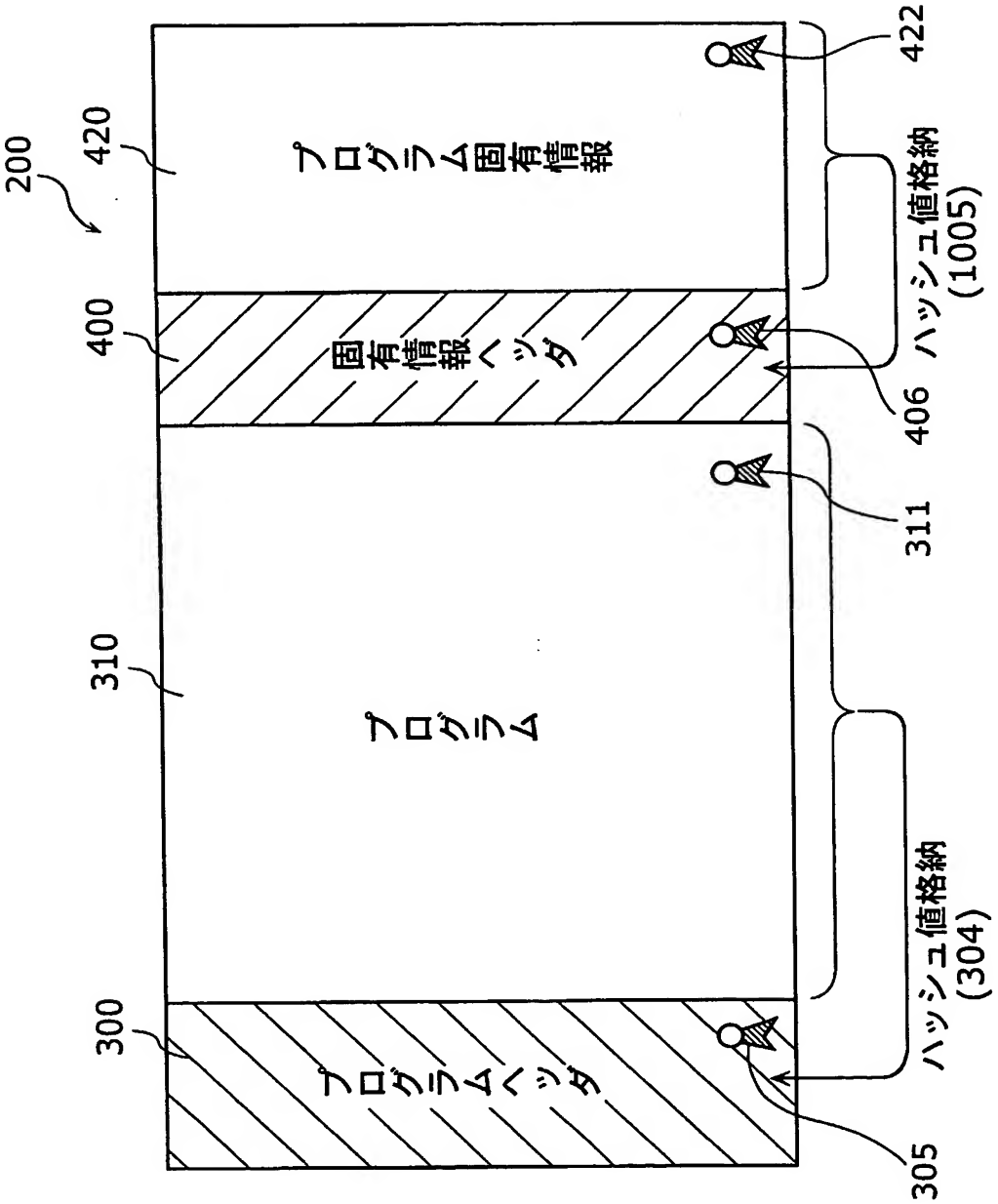

200
420
プログラム固有情報
422
ハッシュ値格納
(1005)
400
固有情報ヘッダ
406
311
310
プログラム
ハッシュ値格納
(304)
300
プログラムヘッダ
305

図3

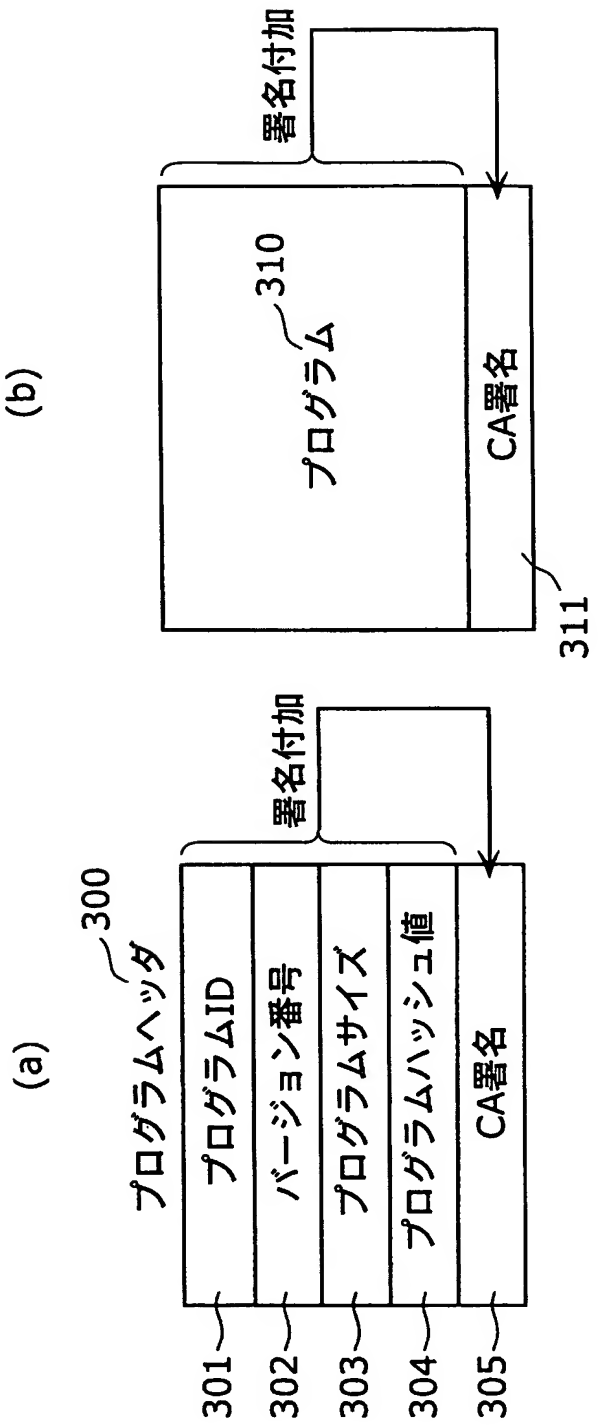

(a)
プログラムヘッダ
300
プログラムID
バージョン番号
プログラムサイズ
プログラムハッシュ値
CA署名
301
302
303
304
305
署名付加
(b)
プログラム
310
CA署名
311
署名付加

図4

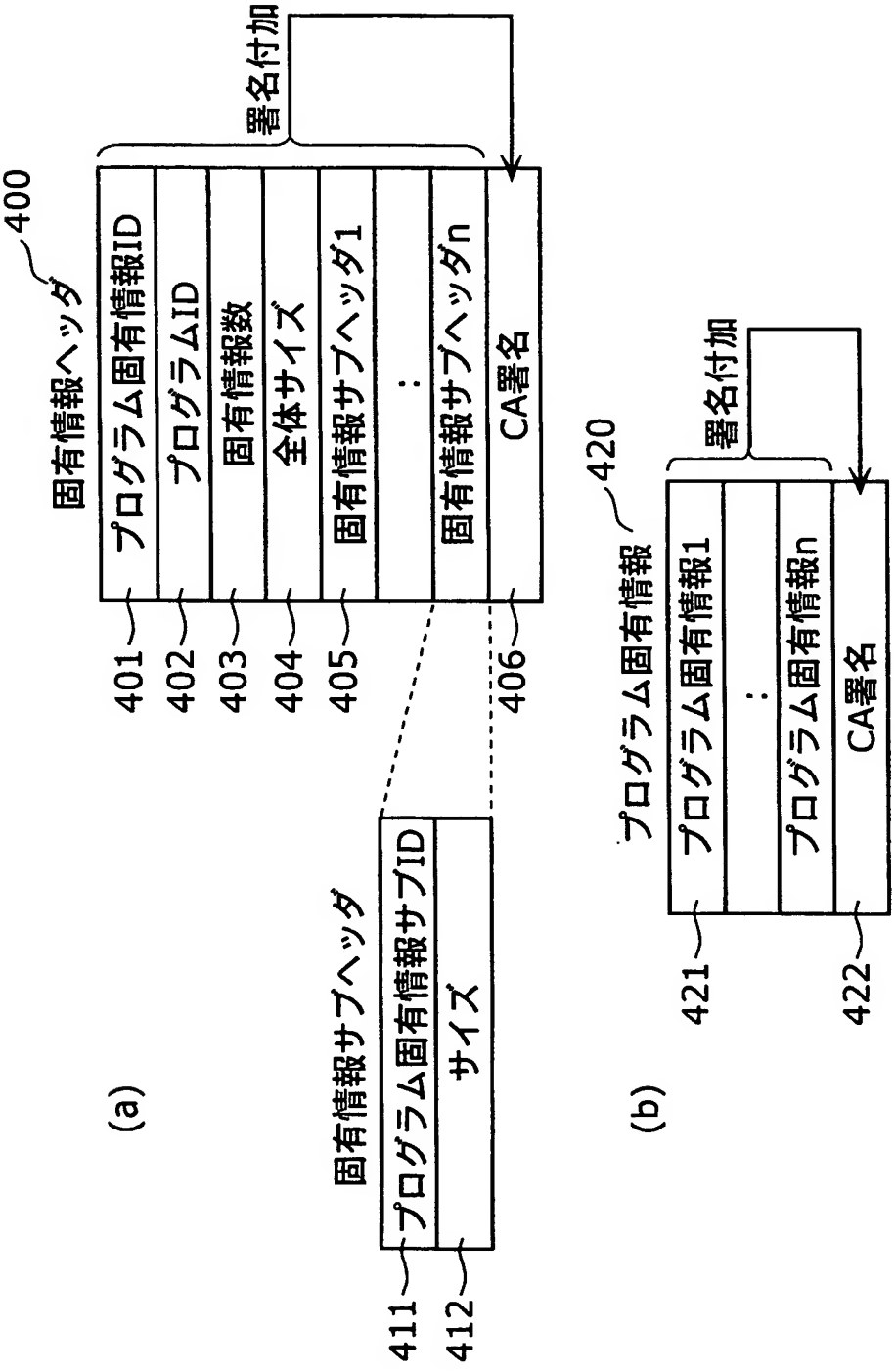

(a)
固有情報ヘッダ
400
プログラム固有情報ID
プログラムID
固有情報数
全体サイズ
固有情報サブヘッダ1
:
固有情報サブヘッダn
CA署名
署名付加
401
402
403
404
405
406
固有情報サブヘッダ
プログラム固有情報サブID
サイズ
411
412
(b)
プログラム固有情報
420
プログラム固有情報1
:
プログラム固有情報n
CA署名
署名付加
421
422

図5

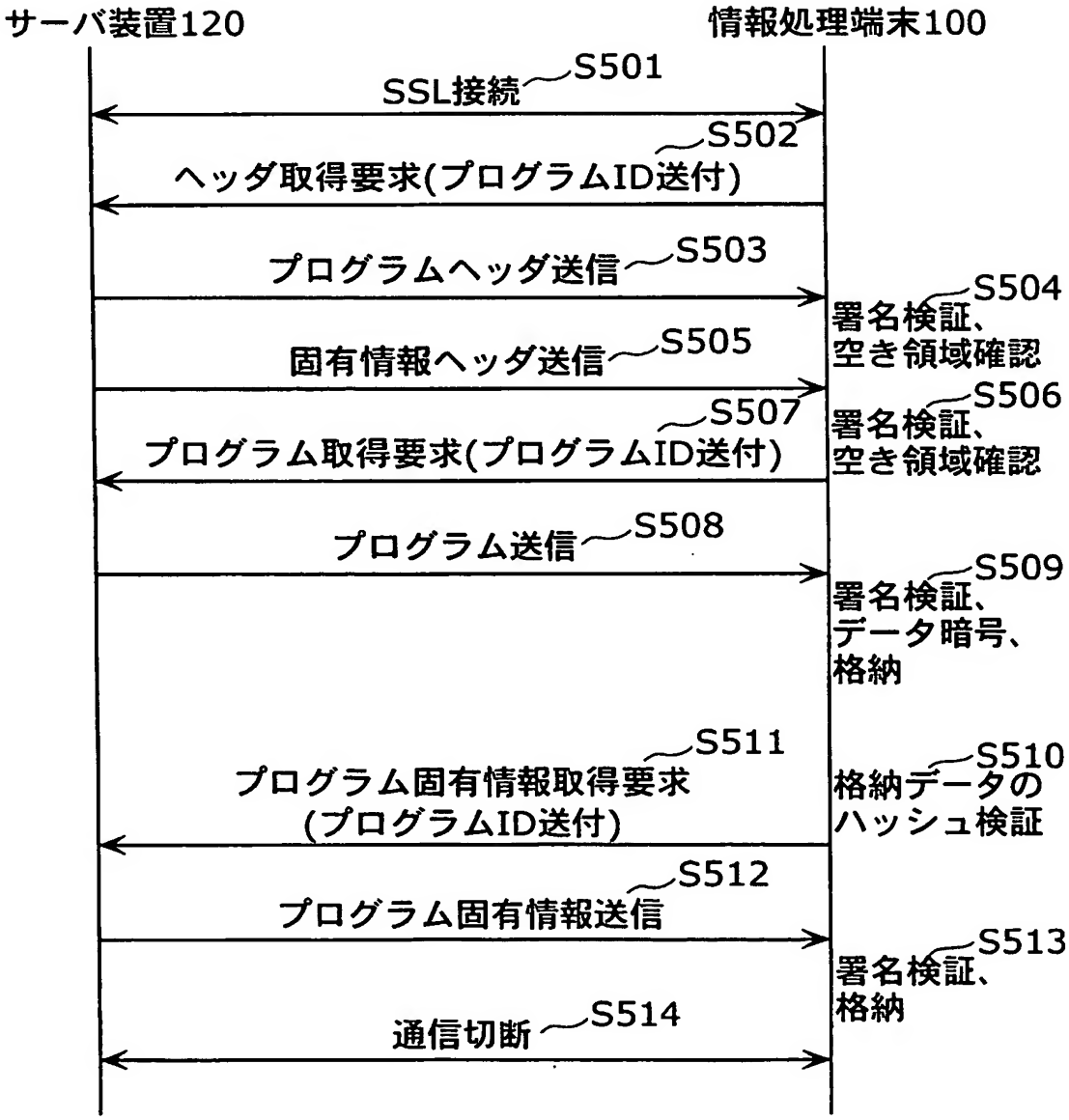

サーバ装置120
情報処理端末100
SSL接続
S501
ヘッダ取得要求(プログラムID送付)
S502
プログラムヘッダ送信
S503
署名検証、
空き領域確認
S504
固有情報ヘッダ送信
S505
署名検証、
空き領域確認
S506
プログラム取得要求(プログラムID送付)
S507
プログラム送信
S508
署名検証、
データ暗号、
格納
S509
プログラム固有情報取得要求
(プログラムID送付)
S511
格納データの
ハッシュ検証
S510
プログラム固有情報送信
S512
署名検証、
格納
S513
通信切断
S514

図6

600

固有情報配布履歴

601 端末ID	602 プログラム固有情報ID	603 最終配布日付
0001	0001	2002.3.12
0002	0002	2002.3.12
0010	0003	2002.3.13
0015	0004	2002.3.14
0020	0005	2002.3.14

図7

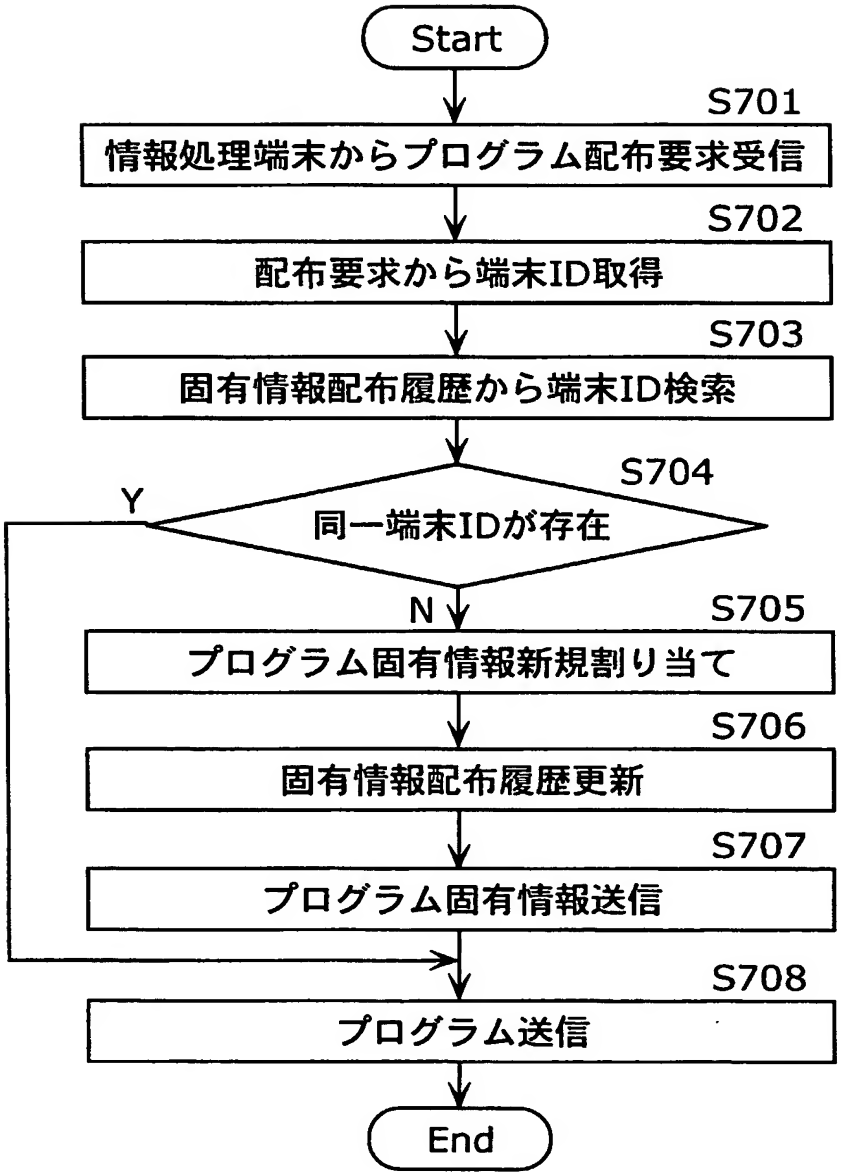

Start
S701
情報処理端末からプログラム配布要求受信
S702
配布要求から端末ID取得
S703
固有情報配布履歴から端末ID検索
S704
同一端末IDが存在
Y
N
S705
プログラム固有情報新規割り当て
S706
固有情報配布履歴更新
S707
プログラム固有情報送信
S708
プログラム送信
End

図8

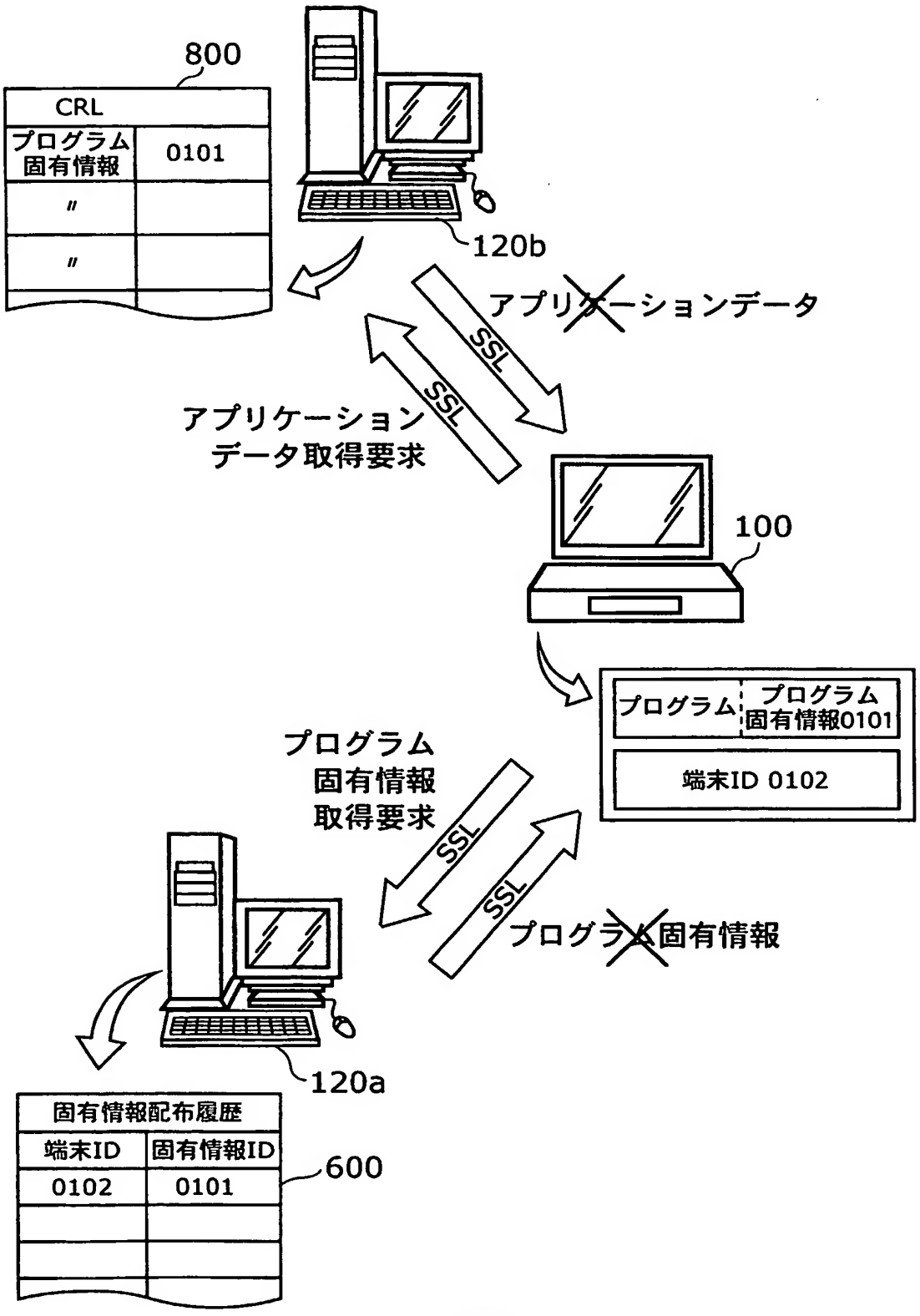

800
CRL
プログラム固有情報
0101
〃
〃
120b
アプリケーションデータ
SSL
SSL
アプリケーションデータ取得要求
100
プログラム
プログラム固有情報0101
端末ID 0102
プログラム固有情報取得要求
SSL
SSL
プログラム固有情報
120a
固有情報配布履歴
端末ID
固有情報ID
0102
0101
600

図9

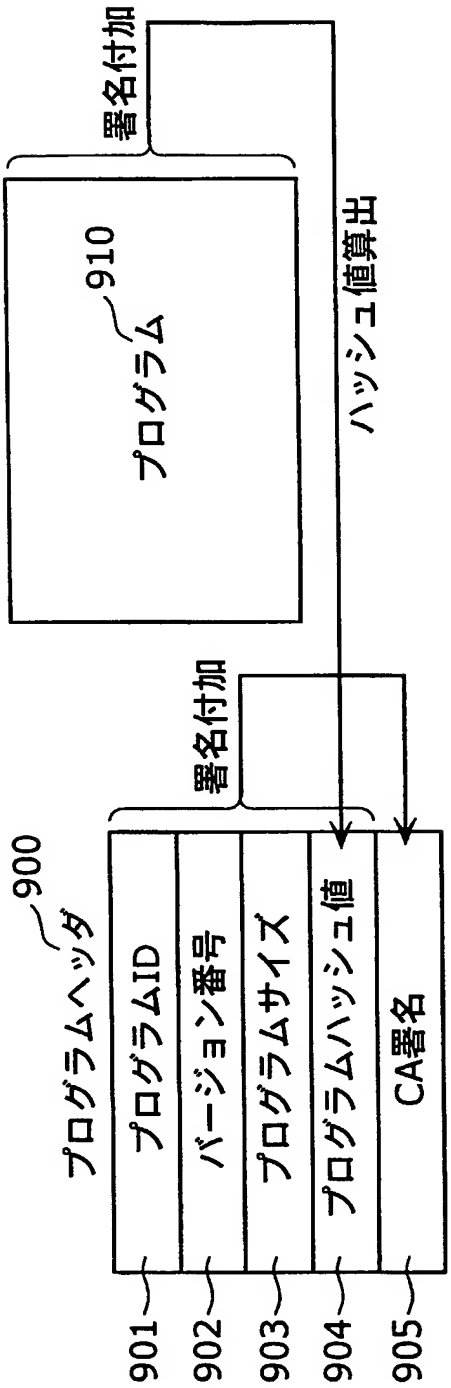

署名付加
910
プログラム
ハッシュ値算出
署名付加
900
プログラムヘッダ
プログラムID
バージョン番号
プログラムサイズ
プログラムハッシュ値
CA署名
901
902
903
904
905

図10

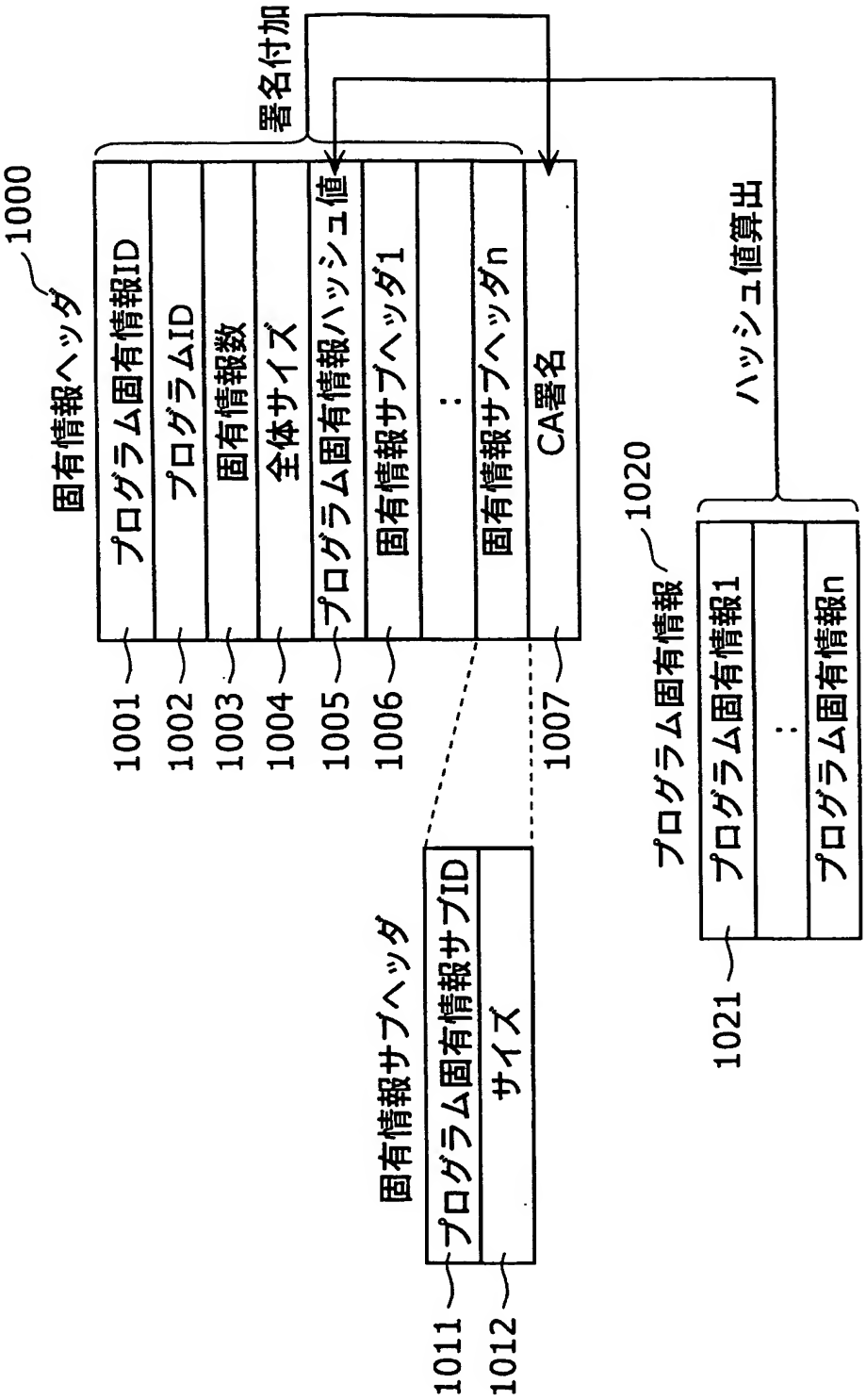

署名付加
1000
固有情報ヘッダ
プログラム固有情報ID
プログラムID
固有情報数
全体サイズ
プログラム固有情報ハッシュ値
固有情報サブヘッダ1
固有情報サブヘッダn
CA署名
1001
1002
1003
1004
1005
1006
1007
ハッシュ値算出
1020
プログラム固有情報
プログラム固有情報1
プログラム固有情報n
1021
固有情報サブヘッダ
プログラム固有情報サブID
サイズ
1011
1012

図11

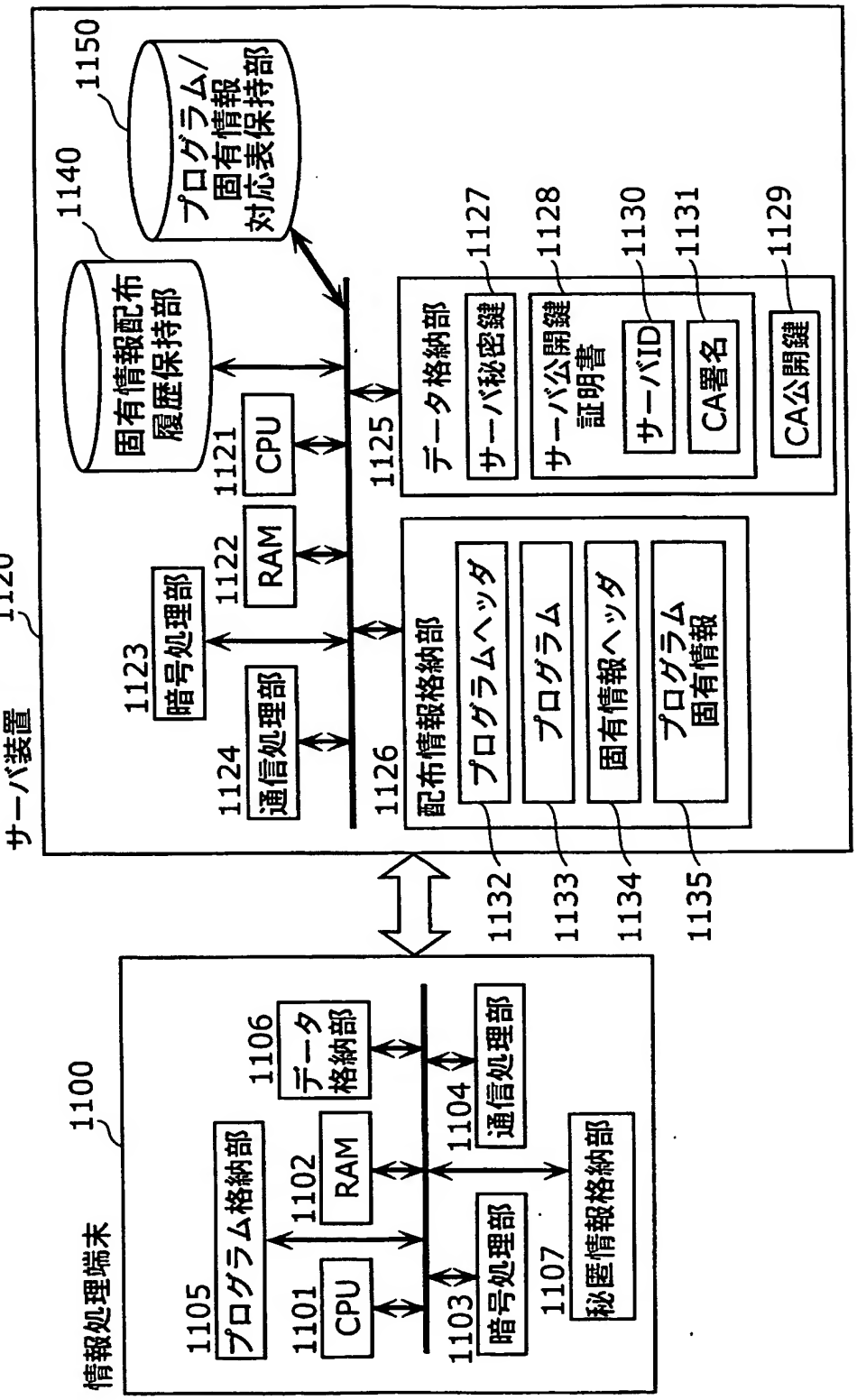

情報処理端末
1100
CPU
1101
RAM
1102
暗号処理部
1103
通信処理部
1104
プログラム格納部
1105
データ格納部
1106
秘匿情報格納部
1107
サーバ装置
1120
CPU
1121
RAM
1122
暗号処理部
1123
通信処理部
1124
配布情報格納部
1126
データ格納部
1125
固有情報配布履歴保持部
1140
プログラム/固有情報対応表保持部
1150
プログラムヘッダ
1132
プログラム
1133
固有情報ヘッダ
1134
プログラム固有情報
1135
サーバ秘密鍵
1127
サーバ公開鍵証明書
1128
サーバID
1130
CA署名
1131
CA公開鍵
1129

図12

(a)

1200

固有情報配布履歴

1201 端末ID	1202 プログラムID	1203 プログラム固有情報ID	1204 最終配布日付
0001	0001	0001	2002.3.12
0002	0001	0002	2002.3.12
0010	0001	0003	2002.3.13
0015	0001	0004	2002.3.14
0020	0002	1001	2002.3.14

(b)

1210

プログラム/固有情報対応表

1211 プログラムID	1212 プログラム固有情報ID	1213 配布開始ID
0001	0001～1000	0123
0002	1001～2000	1423
⋮	⋮	⋮

図13

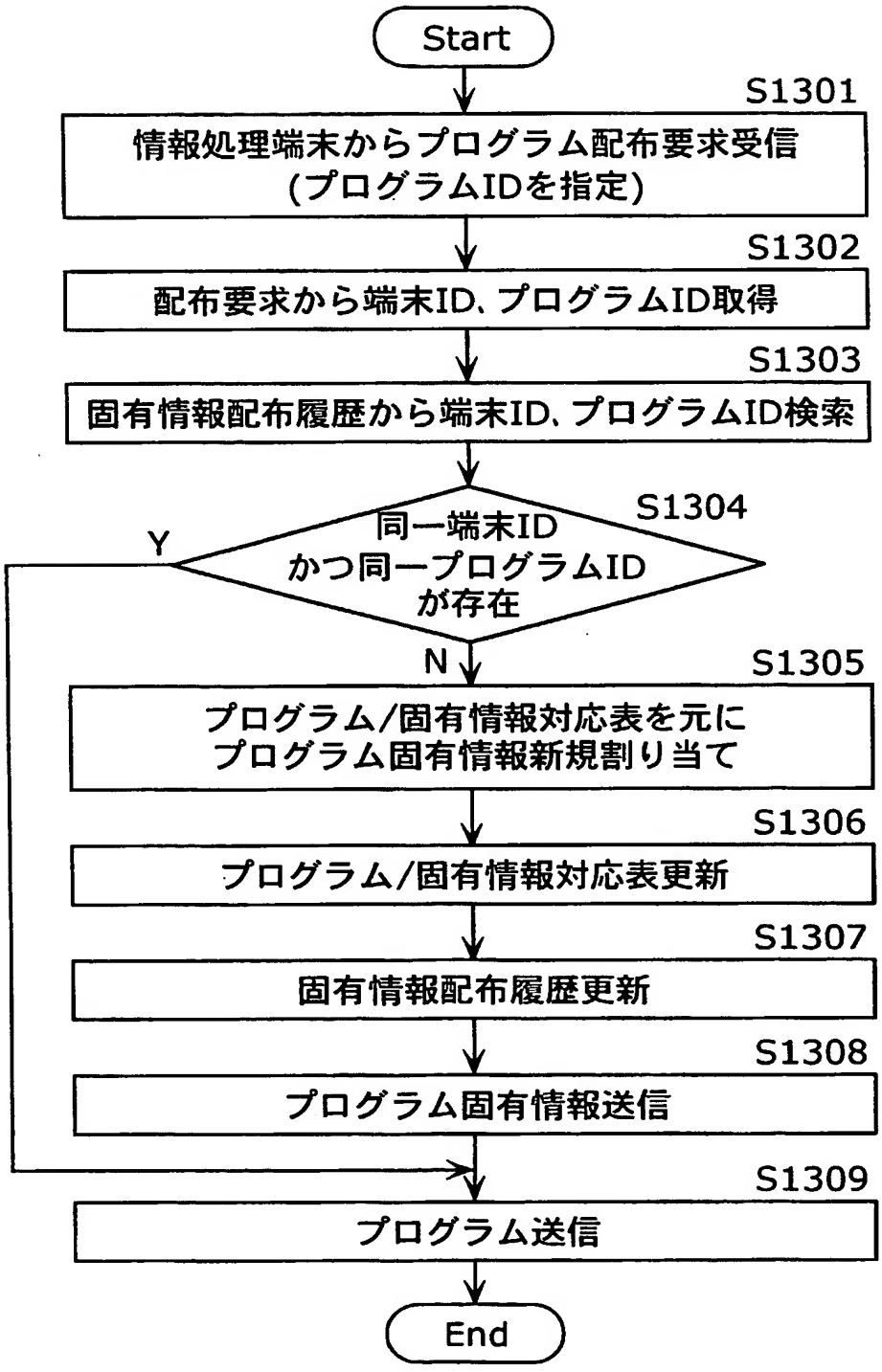

Start
S1301
情報処理端末からプログラム配布要求受信
(プログラムIDを指定)
S1302
配布要求から端末ID、プログラムID取得
S1303
固有情報配布履歴から端末ID、プログラムID検索
S1304
同一端末ID
かつ同一プログラムID
が存在
Y
N
S1305
プログラム/固有情報対応表を元に
プログラム固有情報新規割り当て
S1306
プログラム/固有情報対応表更新
S1307
固有情報配布履歴更新
S1308
プログラム固有情報送信
S1309
プログラム送信
End

図14

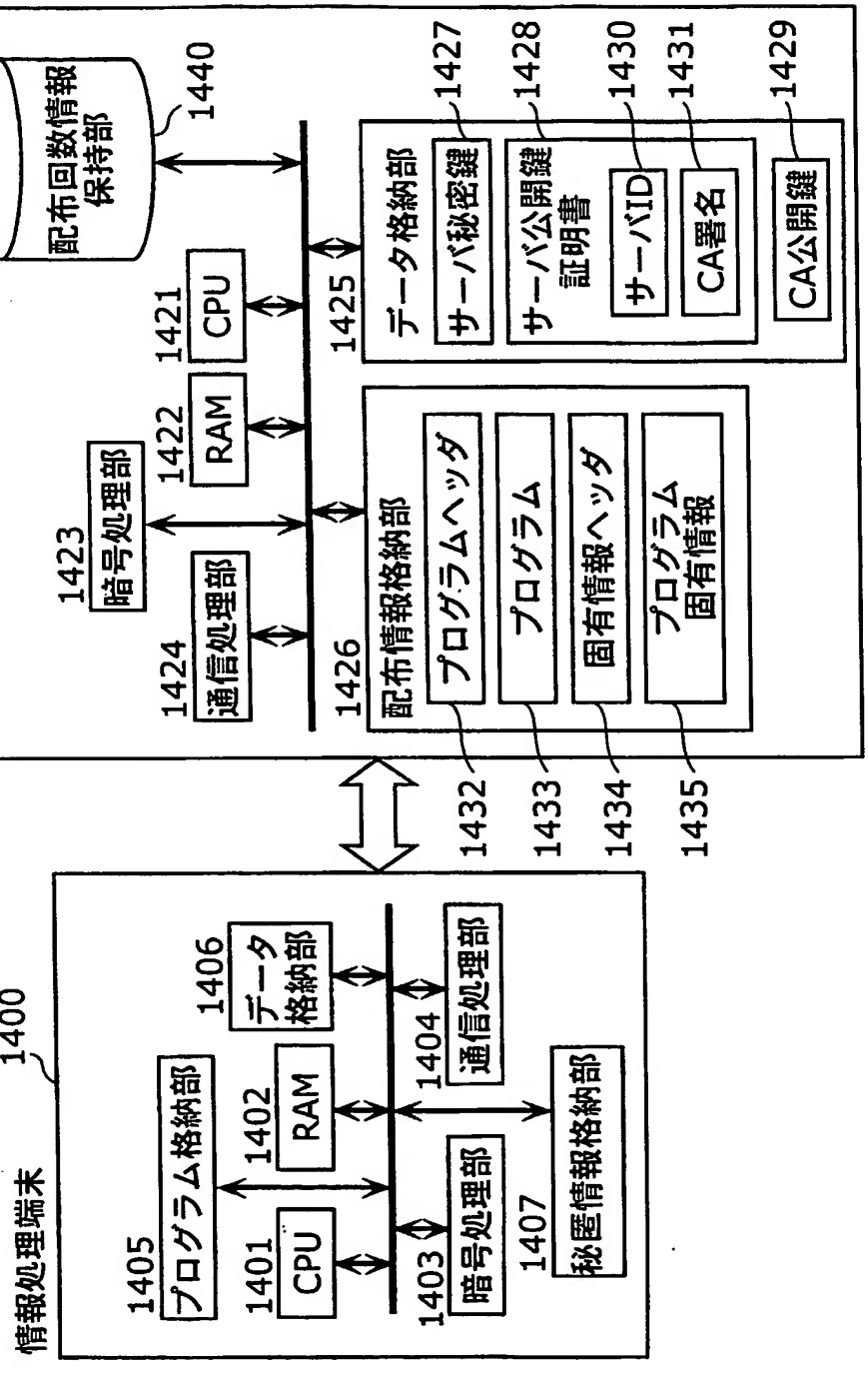

サーバ装置
1420
配布回数情報保持部
1440
CPU
1421
RAM
1422
暗号処理部
1423
通信処理部
1424
1425
1426
配布情報格納部
プログラムヘッダ
プログラム
固有情報ヘッダ
プログラム固有情報
1432
1433
1434
1435
データ格納部
1427
サーバ秘密鍵
サーバ公開鍵証明書
1428
サーバID
1430
CA署名
1431
CA公開鍵
1429
情報処理端末
1400
プログラム格納部
1405
CPU
1401
RAM
1402
暗号処理部
1403
通信処理部
1404
データ格納部
1406
秘匿情報格納部
1407

図15

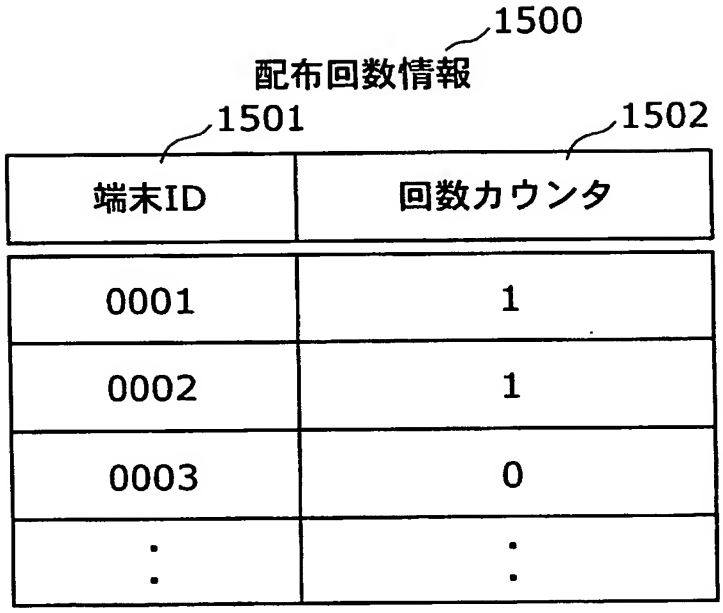


図16

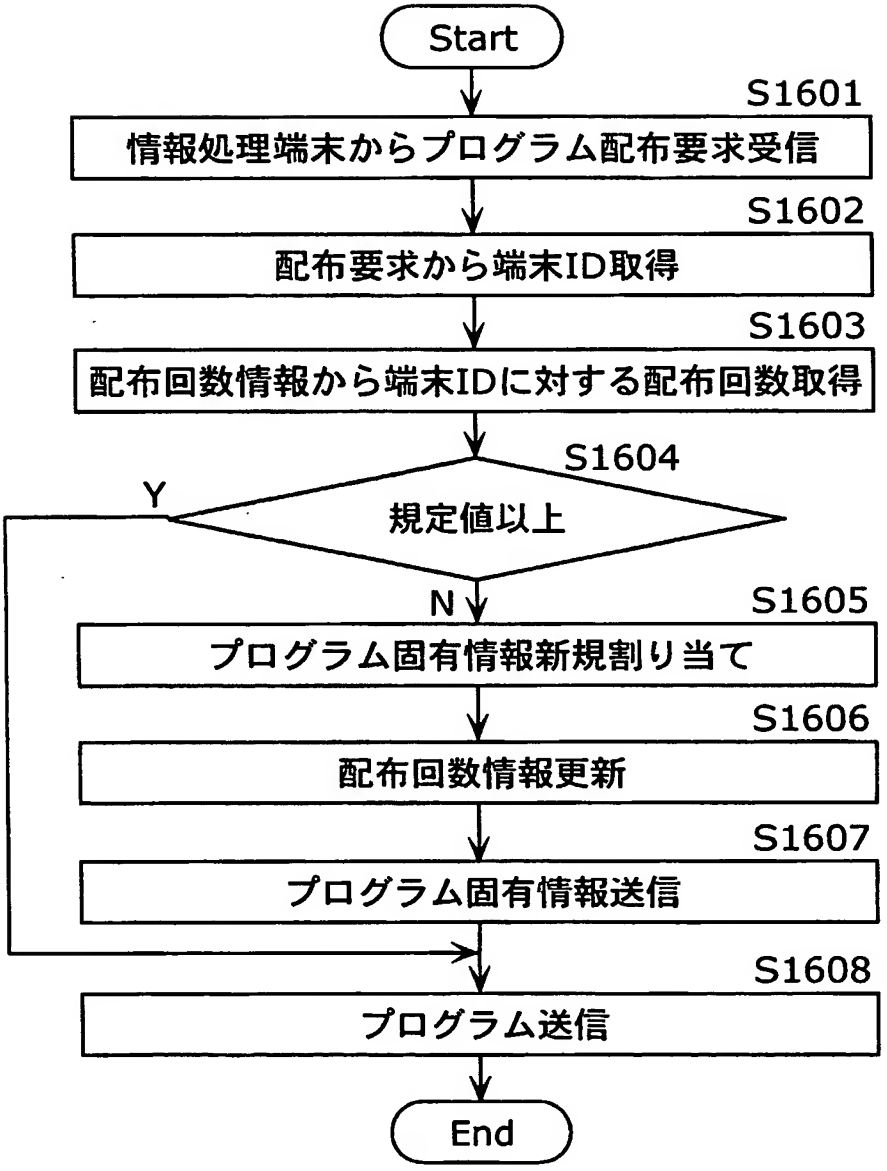

Start
S1601
情報処理端末からプログラム配布要求受信
S1602
配布要求から端末ID取得
S1603
配布回数情報から端末IDに対する配布回数取得
S1604
規定値以上
Y
N
S1605
プログラム固有情報新規割り当て
S1606
配布回数情報更新
S1607
プログラム固有情報送信
S1608
プログラム送信
End

図17

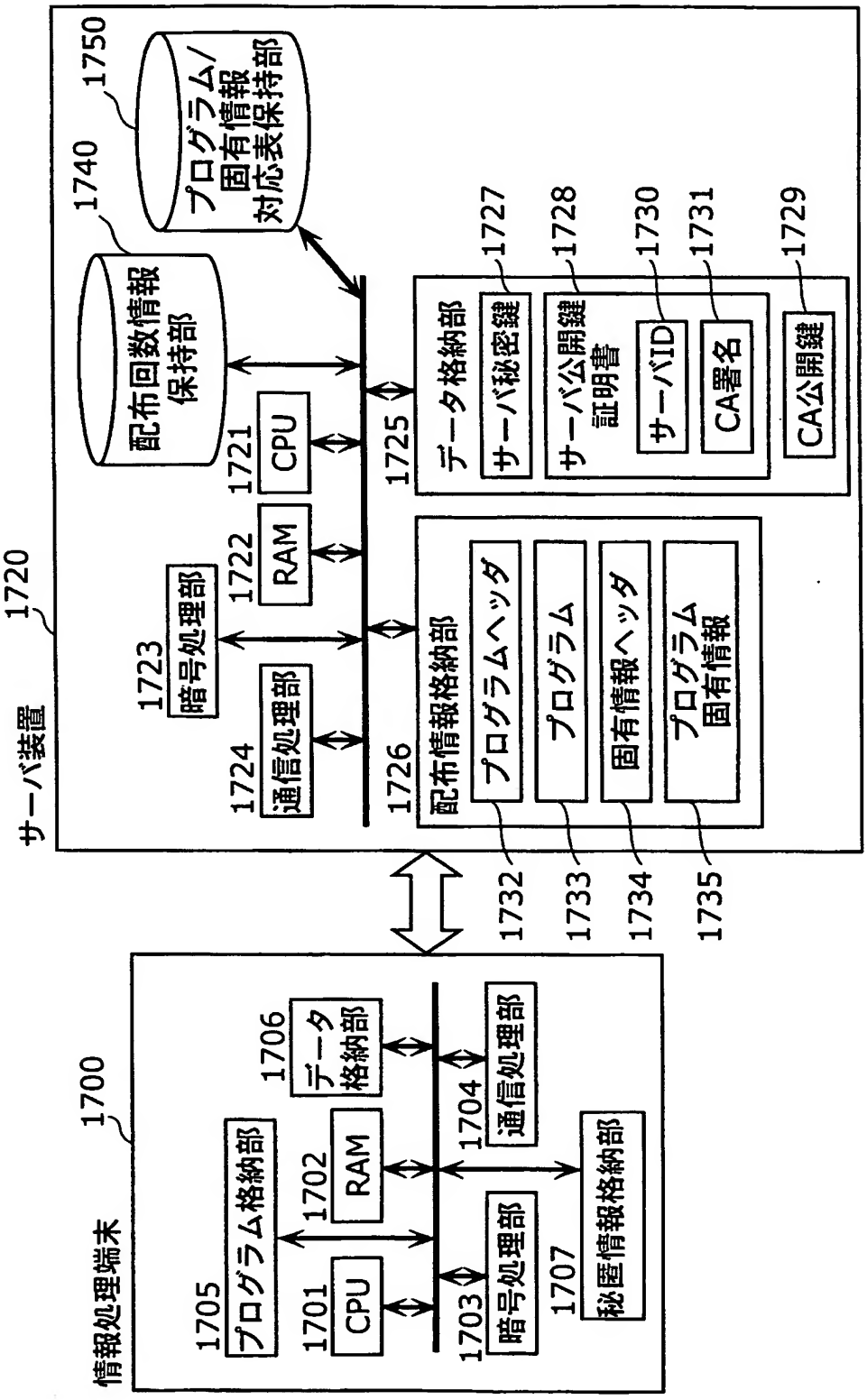

サーバ装置
1720
配布回数情報保持部
1740
プログラム/固有情報対応表保持部
1750
CPU
1721
RAM
1722
暗号処理部
1723
通信処理部
1724
1725
1726
データ格納部
サーバ秘密鍵
1727
サーバ公開鍵証明書
1728
サーバID
1730
CA署名
1731
CA公開鍵
1729
配布情報格納部
プログラムヘッダ
1732
プログラム
1733
固有情報ヘッダ
1734
プログラム固有情報
1735
情報処理端末
1700
CPU
1701
RAM
1702
暗号処理部
1703
通信処理部
1704
データ格納部
1706
プログラム格納部
1705
秘匿情報格納部
1707

図18

(a)

1800
配布回数情報

1801 プログラムID	1802 端末ID	1803 回数カウンタ
0001	0001	1
0001	0002	1
0001	0003	0
0002	0001	1
0002	0002	0
0002	0003	0
⋮	⋮	⋮

(b)

1810
プログラム/固有情報対応表

1811 プログラムID	1812 プログラム固有情報ID	1813 配布開始ID
0001	0001～1000	0123
0002	1001～2000	1423
⋮	⋮	⋮

図19

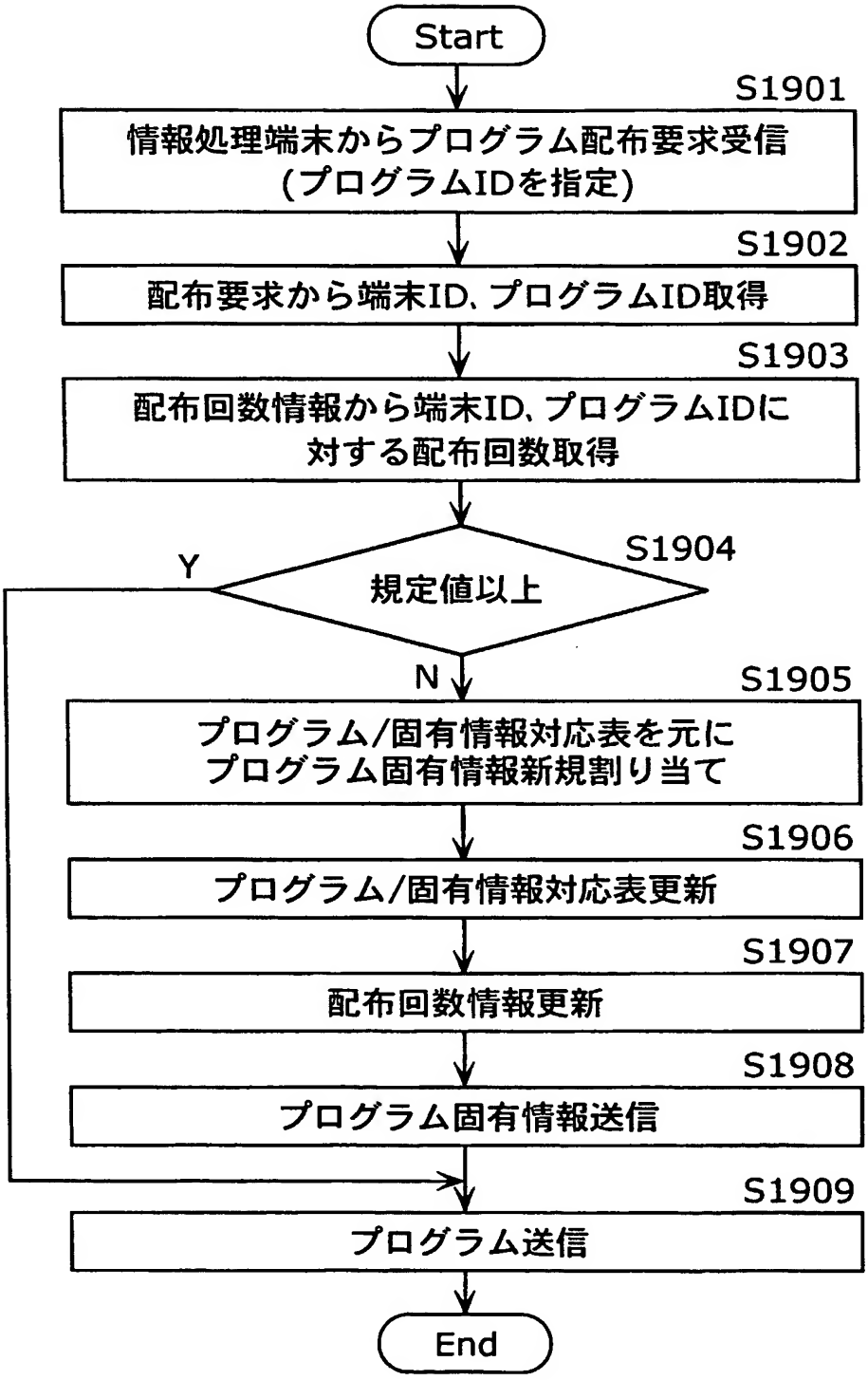

Start
S1901
情報処理端末からプログラム配布要求受信
(プログラムIDを指定)
S1902
配布要求から端末ID、プログラムID取得
S1903
配布回数情報から端末ID、プログラムIDに
対する配布回数取得
S1904
規定値以上
Y
N
S1905
プログラム/固有情報対応表を元に
プログラム固有情報新規割り当て
S1906
プログラム/固有情報対応表更新
S1907
配布回数情報更新
S1908
プログラム固有情報送信
S1909
プログラム送信
End

図20

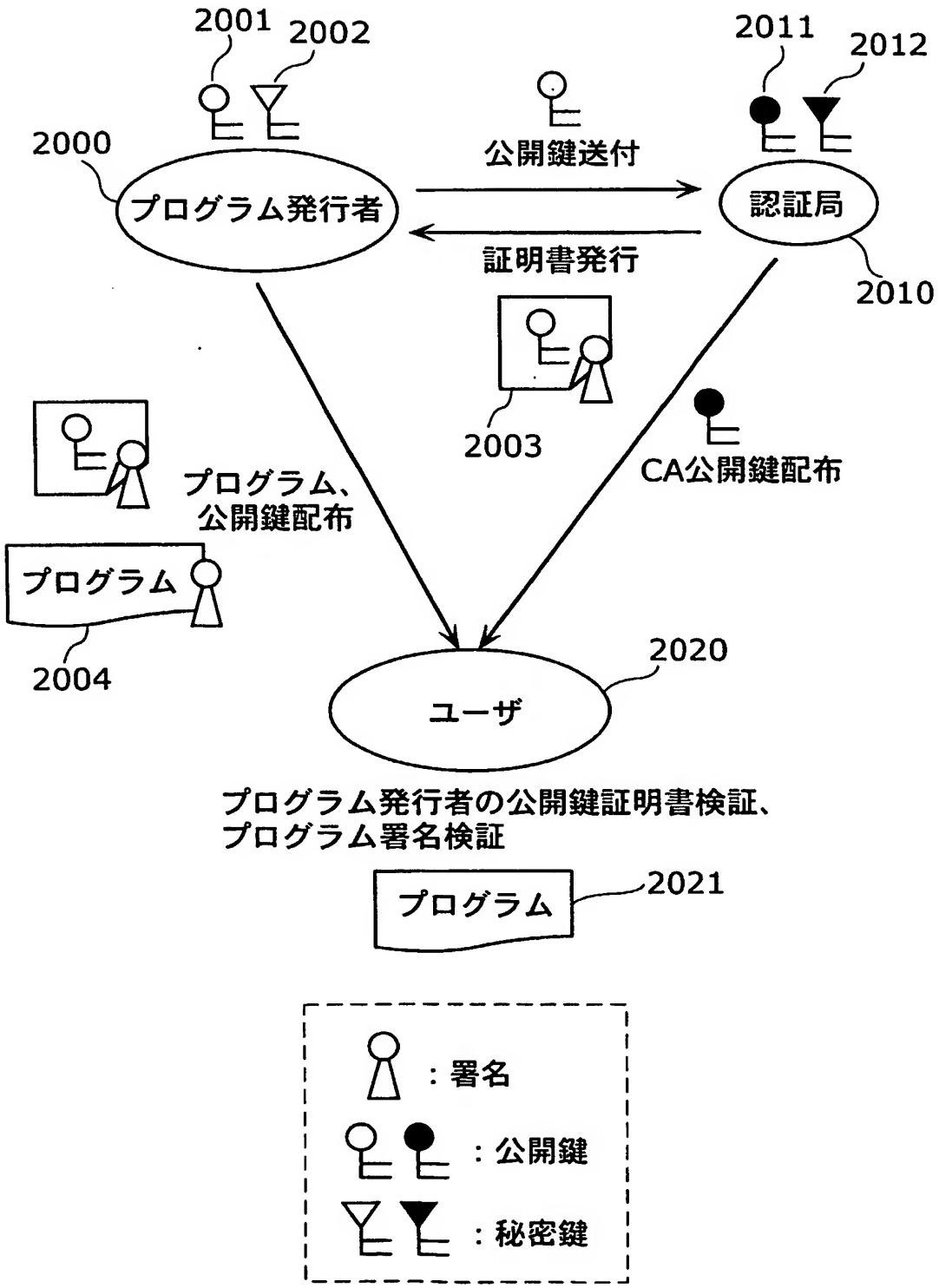
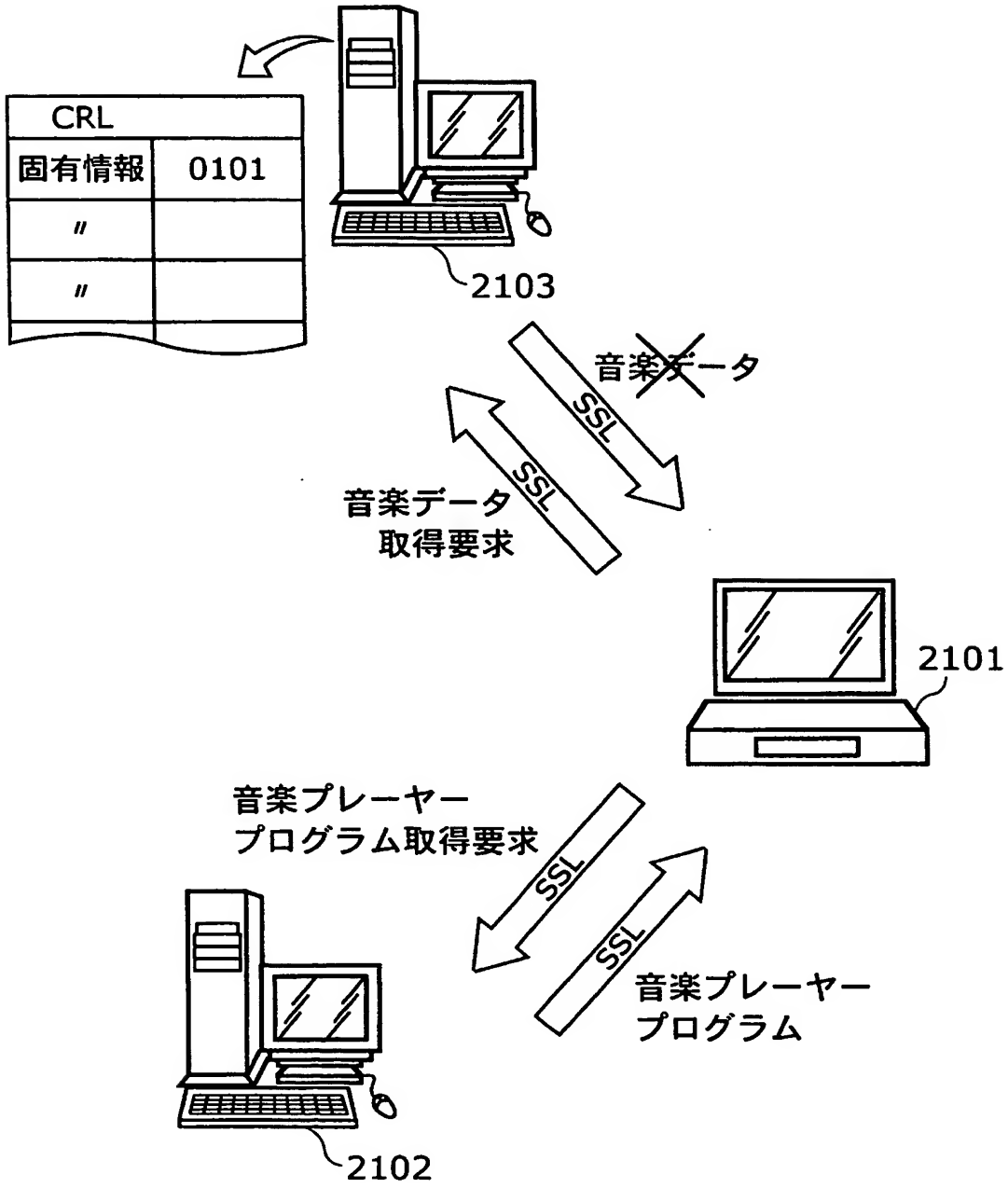

2001
2002
2011
2012
2000
公開鍵送付
プログラム発行者
認証局
証明書発行
2010
2003
CA公開鍵配布
プログラム、
公開鍵配布
プログラム
2004
2020
ユーザ
プログラム発行者の公開鍵証明書検証、
プログラム署名検証
プログラム
2021
：署名
：公開鍵
：秘密鍵

図21


CRL
固有情報
0101
〃
〃
2103
音楽データ
SSL
SSL
音楽データ
取得要求
2101
音楽プレーヤー
プログラム取得要求
SSL
SSL
音楽プレーヤー
プログラム
2102

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/04808

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F1/00, G06F9/445

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F1/00, G06F9/445

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Jitsuyo Shinan Toroku Koho	1996-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Toroku Jitsuyo Shinan Koho	1994-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP 8-190529 A (Fujitsu Ltd.), 23 July, 1996 (23.07.96), Full text; all drawings (Family: none)	1,10,11,16, 17 7 2-6,8,9, 12-15
Y	JP 2000-242491 A (Matsushita Electric Industrial Co., Ltd.), 08 August, 2000 (08.08.00), Full text; all drawings (Family: none)	7
A	JP 2002-91772 A (NEC Corp.), 29 March, 2002 (29.03.02), Full text; all drawings (Family: none)	1-17

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 July, 2003 (29.07.03)	12 August, 2003 (12.08.03)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/04808

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-311083 A (Casio Computer Co., Ltd.), 07 November, 2000 (07.11.00), Full text; all drawings (Family: none)	1-17

国際調査報告

国際出願番号　PCT／JP03／04808

A.　発明の属する分野の分類（国際特許分類（IPC））

Int Cl⁷　G06F1／00, G06F9／445

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int Cl⁷　G06F1／00, G06F9／445

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1926年－1996年
日本国公開実用新案公報　1971年－2003年
日本国実用新案登録公報　1996年－2003年
日本国登録実用新案公報　1994年－2003年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP　8－190529　A（富士通株式会社） 1996．07．23，全文，全図（ファミリーなし）	1, 10, 11, 16, 17
Y		7
A		2-6, 8, 9, 12-15
Y	JP　2000－242491　A（松下電器産業株式会社） 2000．08．08，全文，全図（ファミリーなし）	7

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
29．07．03	12.08.03

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	漆原　孝治	5B	9366
	電話番号　03－3581－1101　内線　3546		

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告　　国際出願番号　PCT／JP03／04808

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP　2002－91772　A（日本電機株式会社） 2002．03．29，全文，全図（ファミリーなし）	1-17
A	JP　2000－311083　A（カシオ計算機株式会社） 2000．11．07，全文，全図（ファミリーなし）	1-17